SG FINSERVE LIMITED (SGFL)

KNOW YOUR CUSTOMER (KYC) GUIDELINES & ANTI-MONEY LAUNDERING STANDARDS (AML) POLICY

VERSION 1.03

Document Title	Know Your Customer (KYC) Guidelines & Anti-Money Laundering Standards (AML) Policy
Effective Date	28th May 2024
Frequency of review	As and when required
Document Owner	Compliance department of the Company
Document Approver	Board of Directors

Contents

1. Preamble

The Reserve Bank of India (RBI) has issued guidelines on Know Your Customer and Anti-Money Laundering and has advised all the NBFC's to ensure that a policy on KYC and AML measures is formulated and approved by the Board of **SG Finserve Limited (SGFL) (Formerly known as Moongipa securities Limited (MSL)** or any another Committee of the Board to which powers has been delegated.

The policy is prepared in line with the RBI guidelines and proposed to be revised with the approval of the Board. The Policy shall be applicable to all the products and services offered by the Company.

2. Know Your Customer Guidelines and Anti-Money Laundering Standards

The objective of the KYC Guidelines is to:

- Adhere to the guidelines issued by RBI in terms of Prevention of Money-Laundering Act 2002, the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 as amended from time to time.
- Adhere to the KYC guidelines issued by RBI as per the Master Direction - Know Your Customer (KYC) Direction, 2016 **(Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 last updated as on 17 October, 2023),** as amended from time to time.
- To prevent company from being used intentionally or unintentionally, by criminal elements for money laundering and terrorist financing activities. KYC procedures also enable Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.
- SGFL's policy framework ensures compliance with PML Act/Rules, including regulatory instructions in this regard and provides a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, SGFL may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

The following four key elements form a part of the policy:

- Customer Acceptance Policy
- Customer Identification Procedures
- Risk Management
- Monitoring of Transactions

3. Definitions

"Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

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

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

"Beneficial Owner" is a natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercise ultimate effective control over a judicial person.

"Certified Copy" - Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Regulated Entity (RE) as per the provisions contained in the Act.
In case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

"Central KYC Records Registry" (CKYCR): Central KYC Registry is a centralized repository of KYC records of customers in the financial sector with uniform KYC norms and inter usability of KYC records across the sector with an objective to reduce the burden of producing KYC documents and getting those verified every time when the customer enters into a new relationship with a financial entity.

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

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

(b) the Managing Partner, if the RE is a partnership firm,
(c) the Proprietor, if the RE is a proprietorship concern,
(d) the Managing Trustee, if the RE is a trust,
(e) a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
(f) a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

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

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

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

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

"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 (43of 1961).

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

"Non-profit organisations" (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as at rust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

"Officially Valid Document" (OVD) means

i. the passport,
ii. the driving licence,
iii. Proof of possession of Aadhaar number,
iv. the 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 and
vi. Letter issued by the National Population Register containing details of name and address.Provided that,

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

Authority of India.

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

I. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
II. Property or Municipal tax receipt;
III. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
IV. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

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

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

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.

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

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

a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e), and
g. Any agency, office or branch owned or controlled by any of the above persons (a to f).

"Politically Exposed Persons" are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Government, senior politicians, senior government/judicial/military officers, senior executive of state-owned corporations, important political party officials.

"Principal Officer" means an officer at the management level nominated by the RE, responsible for furnishing information as per rule 8 of the PML Rules.

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offencespecified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or *bona-fide* purpose; or
d. Gives rise to a reasonable ground of suspicion that it may involve financing of the activitiesrelating 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.

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

a. opening of an account;
b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
c. ;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. Establishing or creating a legal person or legal arrangement.

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

"Correspondent Banking": Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

"Customer" means a person who is engaged in a financial transaction or activity with a

Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

"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 rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

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.

"Customer identification" means undertaking the process of CDD.

"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.

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

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

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

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

"Payable-through accounts": The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

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

"Regulated Entities" (REs) means

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks(RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs /CCBs) and any other entity which has been licenced under Section22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

b. All India Financial Institutions (AIFIs)

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

d. Asset Reconstruction Companies (ARCs)

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

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

"Shell Bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

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

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from timeto time.

4. Designated Director and Principal Officer

Mr. Vivekanand Tiwari, Head-CAD shall act as the Principal Officer of the Company for the purpose of KYC / AML matters and who will be responsible for implementation of and compliance with this policy. His duties, in this regards will be as follows:

- Overall monitoring and compliance of KYC/AML Policy
- Monitoring and reporting of transactions and sharing of information as required under thelaw
- Timely submission of Cash Transaction Reports (CTR's), Suspicious Transaction Reports (STR)or any other applicable reports to FIU-IND
- Submission of periodical reports to management
- Customer Acceptance Policy
- Money Laundering and Terrorist Financing Risk Assessment as per Clause 5A of the RBI-KYCDirections

The **Principal Officer** of the Company shall be appointed as Designated Director for ensuring compliance with the obligations under PMLA, 2002

5. Customer Acceptance Policy

The Customer Acceptance Policy lays down explicit criteria for acceptance of customers. The Policy ensures that the following procedures shall be followed in relation to customer who approach for availing financial facilities with the Company.

- No account is opened in anonymous or fictitious names or on behalf of other persons whoseidentity has not been disclosed or cannot be verified.

- No transaction or account-based relationship is undertaken without following the Customer due diligence procedure. Customer due diligence procedure is to followed for all joint holders, while opening a joint account

- Parameters of risk perception are clearly defined in terms of nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status.

- Customers would be categorized as low, medium and high risk.

- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;

- Not to open an account or close an existing account where the company is unable to apply appropriate customer due diligence measures i.e. company is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the company. The company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

- Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking asthere would be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the

fiduciary capacity.

- Necessary checks will be done before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

- The nature and extent of due diligence will depend on the risk perceived by the company. However, while preparing customer profile, branches/offices should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

- A system is required to be put in place for periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers should be carried out at regular intervals as prescribed by Risk Department of the company.

- Where PAN is obtained, the same shall be verified from verification facility of issuing authority

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

- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

- Where the company forms a suspicion of money laundering or terrorist financing and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

6. Customer Identification Procedure

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. Company need 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 relationship.

1. The first requirement of customer identification procedures to be satisfied is that a prospective customer is the person who he/she claims to be.
2. The second requirement of customer identification procedures is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected or predictable pattern of transactions.

3. Identity shall be verified for:-

    i. The named account holder;
    ii. Beneficial owners;
    iii. Signatories to an account; and
    iv. Intermediate parties.

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

i. While establishing a new business relationship;
ii. Periodically as part of KYC review or when the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

Copies of the documents produced as Proof of Identity and Address shall be obtained and retained with the Company, wherein a responsible Company Official has to attest such copies certifying thatthe Originals thereof have been verified.

The periodicity of updating of customer's identification data should be done once in ten years in case of low risk category customers, once in eight years in case of medium risk category customers and once in two years in case of high risk categories.

Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure-1**.

Also, the information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes. It will be ensured that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his /her consent and after openingthe account.

7. Customer Due Diligence (CDD)

1. Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. 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. Accounts opened using OTP based e-KYC shall not be allowed for more than one year unlessidentification as per Annexure I&II or V-CIP is carried out

3. If Aadhaar details are used for V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

4. The Company may undertake V-CIP to carry out:
   a. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
   b. Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Annexure 1, apart from undertaking CDD of the proprietor.
   c. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication shall be subject to conditions laid down in Master Directions, updated from time to time.
   d. Updation/Periodic updation of KYC for eligible customers.

5. While undertaking V-CIP, SGFL adhere to minimum standards as mentioned in Annexure IV.

6. In case the CDD is outsourced, then the records or the information of the customer due diligence carried out by the third party should be obtained within reasonable time from the third party or from the Central KYC Records Registry.

7. In case the CDD is outsourced, the decision making functions of determining compliance with KYC norms should not be outsourced.

8. CDD procedure should be applied at the UCIC level and if an existing KYC complaint customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

9. CDD procedure shall be followed for all joint account holders, while opening a joint account.

10. The Company can establish relationship with Politically Exposed Persons (PEPs) provided that
    a. Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
    b. the identity of the person shall have been verified before accepting the PEP as a customer;
    c. the decision to open an account for a PEP is taken at a senior level in accordance with the Company's Customer Acceptance Policy; senior level for this purpose shall include HOD & above.
    d. all such accounts are subjected to enhanced monitoring on an on-going basis;
    e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

    The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

8. Risk Management

The Company shall adopt a risk-based approach to ensure that an effective KYC programme is put inplace by establishing appropriate procedures and ensuring their effective implementation. Company will adhere to the following for effective implementation of Risk Management:

a. Originals of the KYC documents shall be verified by officials of the Company and copies thereof shall be obtained and retained with the Company. Such copies shall be attested by the Company officials certifying that they have been verified with the originals.
b. KYC documents so obtained shall be properly arranged and filed in order so that they shall be available for verification any time.
c. Company's Internal Auditors shall ensure an independent evaluation of compliance of KYC/AML policy including legal and regulatory requirements. They shall report Lapses observed in this regard as Irregularities in their Audit Reports.
d. Adverse features noted by the Internal Auditors shall be brought to the attention of the Principal Officer.
e. Summary of serious Irregularities/deviations shall be placed before the Audit Committee ofthe Board by the Internal Audit Department at quarterly intervals.
f. Review of implementation of KYC/AML guidelines shall also be placed before the Audit Committee of the Board by the Principal Officer at quarterly intervals.
g. The Company shall have an on-going employee training programme so that members of thestaff are adequately trained in KYC/AML procedures.
h. The Principal Officer designated by the Company in this regard shall have responsibility in managing oversight and coordinating with various functionaries in the implementation of KYC/AML Policy.
i. Designated Director shall be responsible for the overall compliance with the obligations under the Act and Rules.

9. Risk Categorization

The Company shall categorize its customers based on the risk perceived by the Company. The levelof categorization would be Low risk, Medium Risk and High risk.

I. Risk categorization 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, 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.

II. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

III. For the purpose of risk categorization, individuals and entities whose identities and

source of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as **low risk**. Examples of low risk customers would be people belonging to lower economic strata of the society whose accounts show small balances and low turnover, government departments, government owned companies, statutory bodies, and salaried individuals.

IV. Customers who are likely to pose higher than average risk to the Company would be categorized as medium or high risk. While categorizing the customers are medium or high risk due consideration would be given to customer's background, nature of activity, country of origin, and profile etc. In such cases, Company will apply higher due diligence measure keeping in view the risk level. Examples of customer requiring higher due diligence may include non- resident customer, trusts, societies, charitable organization, non-face to face customers, those with dubious reputations as per public information available etc. Characteristics of High Risk and Medium Risk Customers is given as **Annexure 3**.

V. Special care and due diligence shall be exercised in case of individuals who happen to be Politically Exposure Persons (PEP). PEP are individuals who are or have been entrusted with prominent public functions within or outside the country like Heads of States/Government, senior politicians, senior government/judicial/military officers, senior executive of state- owned corporations, important political party officials etc

VI. Full KYC exercise will be required to be done at least **every two years for high risk** individuals and entities.

VII. Full KYC exercise will be required to be done at least **every eight years for medium risk** and at least **every ten years for low risk** individuals and entities taking in to account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.

VIII. If an existing KYC compliant customer desires to open another account with the Company there should no need for submission of fresh proof of identity and/or proof of address for the purpose.

IX. Fresh photographs will be required to be obtained from minor customer on becoming major.

10. Monitoring of Transactions:

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent logical or visible lawful purpose Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer will be subjected to detailed scrutiny.

After due diligence at the appropriate levels in the company, transactions of suspicious nature and/or any other type of transaction notified under PML Act, 2002 will be reported to the

appropriate authority and a record of such transaction will be preserved and maintained for a period as prescribedin the Act.

11. Beneficial Ownership

The Company shall determine the beneficial ownership and controlling interest in case of the customers who are not individuals and the KYC of the beneficial owners will be completed. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice. The guidelines applicable for Beneficial Ownership is given as **Annexure II.**

12. Unique Customer Identification Code

Every customer should be provided with a Unique Customer Identification Code. This will help to identify customers, track the facilities availed, monitor financial transactions and enable the Company to have a better approach to risk profiling of customers.

13. Internal Control System

a) The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

b) The Management under the supervision of Board shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the application of KYC procedures at the branches and comment on the lapsesobserved in this regard.

c) The compliance in this regard shall be put up before the Audit Committee of the Board along with their normal reporting frequency.

d) Further, the HR Department of the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel called as the KYE (Know Your Employee) so as to ensure that persons of criminal nature/ background do not get an access, to misuse the financial channel.

14. Record Management

Maintenance and Preservation of records

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

b. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years afterthe business relationship is ended;

c. make available swiftly, the identification records and transaction data to the

competent authorities upon request;

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

i. All cash transactions of the value of more than Rs.10 lakhs or its equivalent in Indian currency, though by policy the Company does not accept cash deposits in foreign currency shall be supported by the PAN of the customer.

ii. PAN number to be collected by the branch for all series of cash transactions integrally connected to each other which have been valued above Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.

iii. All transactions involving receipts by non-profit organizations of Rs.10 lakhs or itsequivalent in foreign currency.

iv. 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 has taken place; any such transactions.

v. All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.

(vi) all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;

(vii) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

e. Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as topermit reconstruction of individual transaction, including the following:

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it was denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction.

f. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

g. Maintain records of the identity and address of their customer, and records in

respect of transactions referred to in Rule 3 in hard or soft format.

Explanation. – For the purpose of this Section, 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.

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

15. Customer Education

The Company recognizes the need to spread the awareness of KYC/AML measures and the rationale behind them amongst the customers. Appropriate measures will be taken in this regard.

16. Periodic Updation (KYC in Existing Accounts)

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers. The time limits prescribed above would apply from the date of opening of the account/last verification of KYC.

Details pertaining to type of customers & periodic updation is appended below:

a. **Individual Customers:**

No change in KYC information

In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of the Company), letter etc.

Change in address

The Company shall have the following options for updates pertaining to change in address:

1. In case of a change only in the address details of the customer, a self-declaration of thenew address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of the Company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

2. The Company, shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer

at the time of periodic updation.

3. The Company may use "Aadhaar OTP based e-KYC in non-face to face mode" for periodic updation. It is crucial to emphasize that the conditions outlined in Section 17 of Master Direction - Know Your Customer (KYC) Direction, 2016 do not apply when conducting updation or periodic updation of KYC through Aadhaar OTP-based e-KYC in the non-face to face mode.

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

b. Customers other than individuals:

No change in KYC information

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

Change in KYC information

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

c. Additional measures:

In addition to the above, the Company shall ensure that

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

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

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC

are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, the Company has the facility of periodic updation of KYC at any branch.

v. The Company shall ensure that adverse actions against the customers shall be avoided, unless warranted by specific regulatory requirements.

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

In case of existing customers, the Company shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which the Company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer. Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard.
Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation to an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the provisions of this Section. For the purpose of ceasing the operation in the account, only credits shall be allowed. Also, additional disbursement and/or top-up loans shall be ceased.

For customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes, the Company make attempts to receive the requisite documents. The Company, at its discretion, may extend a relaxation of up to 3 months to the customer. Such accounts shall, however, be subject to enhanced monitoring.

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

The Company shall continue engaging with its customers for having their KYC updated in such cases.

17. Introduction of New Technologies

Company will pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent misuse of technology innovations for money laundering activities. Company will ensure that appropriate KYC procedures are duly applied to customers using new technology driven products.

18. Persons Authorized

The Company shall accept full consequences of any violation by the persons authorized including brokers/agents etc. who are operating on its behalf.

19. Prevention of Money Laundering Act, 2002 – Obligations of Company in terms of rules notified thereunder

Company has appointed "Principal Officer" who will put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. Further with the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

"If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

a. Issue a warning in writing; or

b. Direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

c. direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

d. By an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

For the purpose of this policy document, the term 'money laundering' would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of funds.

1. Money Laundering - Risk Perception

Following are the risks, which arise out of Money Laundering activities:

a. Reputation Risk - Risk of loss due to severe impact on reputation. This may be of particular concern given the nature of business, which requires the confidence of customers, and the general market place.

b. Compliance Risk - Risk of loss due to failure of compliance with key regulations governing the operations.

c. Operational Risk - Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

d. Legal Risk - Risk of loss due to any legal action on company or its staff may face due to failure to comply with the law.

Company should ensure to cover all the above stated risks and should have proper checks to controlto combat the above stated risks.

2. Maintenance of Records of Transactions and Preservation

There will be a system of maintaining proper record of transactions prescribed under PMLA, 2012 and PML Rule 2005 in prescribed format. The same along with KYC documents should be preserved for prescribed period. The Company will hire vendors where the physical copies will be preserved and also important data will be kept online on computer servers.

3. Reporting to Financial Intelligence Unit - India

Company will abide the PMLA rules for reporting information pertaining to cash and suspicious transactions to the specified authorities post conducting due enquiries. As a part of transaction monitoring mechanism, systems/ processes will be put in place to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

The periodical reporting to FIU will be done regularly in soft copy through online mode. For e.g. CTRfiled online on FIU website on regular basis.

4. Suspicious Transaction Monitoring and Reporting

NBFCs are required to file reports on suspicious transactions with financial intelligence unit – India (FIU), as per the prevention of Money Laundering Act (PMLA), within seven days of a transaction getting identified as a suspicious transaction by the principal officer (PO). The suspicious transaction is defined by RBI as a transaction, including as attempted transaction, whether or not made in cash, which to a person acting in good faith:

- Gives rise to a reasonable ground of suspicion that it may involve proceeds of anoffence specified in the Schedule to the Act, regardless of the value involved ; or
- Appears to be made in circumstances of unusual or unjustified complexity; or
- Appears to not have economic rational or bona – fide purpose; or
- Gives rise to a reasonable ground of suspicion that it may involve financing of theactivities relating to terrorism.

Monitoring and Reporting of Suspicious transaction activity
The Company will keep a continuous vigil with regards to customers behavior or approach while dealing with the company. The company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no

apparent economic or visible lawful purpose.

In case any usual act or event or behavior is noticed in relation to customer, the same shall be investigated and if required report as suspicious activity. The staff of branches / department should observe the traits of customer that raise suspicion. List of suspicious transactions to be tracked is given below:

- Reluctance on part of the customer to provide confirmation regarding his identity, nature of business, business relationship, officers or directors or its locations
- KYC documents provided by the customer are forged, fabricated or altered
- KYC documents provided by the customer cannot be verified (e.g foreign documents)
- Forged documents provided by the customer (e.g. fake title deeds)
- Difficulty in identifying beneficial owner of the transaction
- Nature of transaction under taken by the customer is too complex or the customer is not able to explain the source of funds
- Nature of transaction undertaken by the customer does not justify his nature of business or lifestyle or standard of living
- Customer has limited or no knowledge about the money involved in transaction or conducting transaction on behalf of someone else
- Customer is investigated for criminal offence by law enforcement agency
- Customer is investigated for terrorist financing or terrorist activities
- Adverse media report about the customer
- Negative Information about the customer received from any other financial institution (e.g. fraud etc)
- For all part prepayments/ foreclosures which are not balance transfer (BT) involving Rs. 0.50 Crs. or above should be reviewed through customer service and reported to Principal Officer. The Risk team shall review whether same is suspicious or not and accordingly Principal Officer shall report the same if required.

Any enquiry from CBI, Police, Enforcement Directorate, Department or Vigilance and Anti-corruption, Income Tax or Service tax authorities etc about the statement of account of the customer should result in STR.

Monitoring and Reporting of Cash Transactions

No cash of Rs. 50,000/- and above shall be accepted from a Customer/ any other intermediary (auction cases) without obtaining a copy of the PAN card of the Customer/any other intermediary. In case a Customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

Any cash transactions of Rs. 10 lakhs and above and integrally connected cash transactions of Rs, 10 lakh and above per month shall be reported to **FIU-IND by 15th of the succeeding month as CTR. For further details, Rules 3 to 8 (Appendix B) may be seen**.

The Company shall lay down proper mechanism to check any kind of attempts to avoid disclosure of PAN details. In case of possible attempts to circumvent the requirements, the same shall be reviewed from the angle of suspicious activities and shall be reported to FIU-IND, if required.

20. Central KYC Records Registry

Government of India has authorized the Central Registry of Securitization 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.

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.

SGFL 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.

SGFL shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

SGFL shall upload the KYC data pertaining to all new individual accounts opened on or after its operations, with CKYCR in terms of the provisions of the Rules ibid.

Once KYC Identifier is generated by CKYCR, SGFL shall ensure that the same is communicated to the individual/LE as the case may be.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, SGFL shall upload/update the KYC data pertaining to accounts of individual customers after starting its operations and at the time of periodic updation as specified in the Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

SGFL shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

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

a. there is a change in the information of the customer as existing in the records of CKYCR;

b. the current address of the customer is required to be verified;

c. The SGFL considers it necessary in order to verify the identity or address of the

customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

21. Combating financing of Terrorism

1. Company shall institute suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.
2. Before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs).
3. It would be necessary that adequate screening mechanism is put in place by Company as an integral part of their recruitment/hiring process of personnel.
4. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions.

22. Annexures

Annexure I - Indicative list of documents for Customer Due Diligence (CDD)

Sr. No.	Individual / Type of Entity (features to beverified)	Documents required
1.	Individuals	Permanent Account Number (Mandatory) (the same shall be verified from the verification facility of theissuing authority including through DigiLocker) AND Any one of the OVD (Proof of Identity and Address) AND One recent photograph **List of OVD:** i. the passport, ii. the driving licence, iii. Proof of possession of Aadhaar number, iv. the Voter's Identity Card issued by the ElectionCommission of India, v. Job card issued by NREGA duly signed by an officerof the State Government and vi. Letter issued by the National Population Registercontaining details of name and address.

		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. 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. Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:- i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. Property or Municipal tax receipt; iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; Customer shall submit OVD with current address within a period of three months of submitting the documents specified above
2.	Proprietorship Concerns	Documents or equivalent e-documents which could be obtained as proof of business/activity for proprietary firms (any two) in additions to the documents of the proprietor as individual: a. Registration certificate including Udyam Registration Certificate (URC) issued by the Government b. Certificate/licence issued by the municipal

		authorities under Shop and Establishment Act. c. Sales and income tax returns. d. GST certificate (provisional / final) e. Certificate /registration document issued by Sales 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 their discretion, accept only one of those documents as proof of business/activity. Provided that it undertakes contact point verification and collects such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
3.	Company Name of the Company Principal place of business Mailing Address Telephone No.	Certified copies of following documents or equivalent e-documents should 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) Individual KYC of person authorized to transact on behalf of the company (f) The name of the relevant persons holding senior management position; and (g) The registered office and the principal place of its business, if it is different.

4.	Partnership Firms Legal Name Address Names of all partners andtheir address Telephone No.	Certified copies of following documents or equivalent e-documents should be obtained: (a) Registration certificate (b) Partnership deed (c) Permanent Account Number of the partnership firm (d) Individual KYC of person authorized to transact on behalfof the 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.
5.	Trust Name of Trust / Trustees /Settlors / beneficiaries / Signatories / founders Telephone No.	Certified copies of following documents or equivalent e-documents should be obtained: (a) Registration certificate (b) Trust deed (c) Permanent Account Number or Form No.60 of the trust (d) Individual KYC of person authorized to transact on behalfof the firm (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 Individual KYC documents for those discharging the role as trustee and authorized to transact on behalf of the trust.
6.	Unincorporated Association / Body of Individuals (Includes Unregistered Trusts / Partnership Firms / Societies)	Certified copies of following documents or equivalent e-documents should be obtained: a. Resolution of the managing body of such association orbody 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. Individual KYC of person authorized to transact on behalf ofthe firm e. Any other information/document as may be required to collectively establish the legal existence of such an association or body of individuals.

7.	Others	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 equivalent e-documents shall be obtained and verified: (a) Document showing name of the person authorized to acton behalf of the entity; (b) Individual KYC of person authorized to transact on its behalf (c) Any other information/document as may be required to establish the legal existence of such an entity/juridical person

Annexure II – Beneficial Owners

Sr. No.	Applicable for	Guidelines	
1.	Company	the beneficial owner is the natural person(s), who , whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.	"Controlling ownership interest" means ownership of/entitlement to **more than 10 per cent** of the shares or capital or profits of the company "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
2.	Partnership Firm	Beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to **more than 10 per cent** of capital or profits of the partnership or who exercises control through other means. Explanation – for the purpose of this sub-clause, "control" shall include the right to control the management of policy decision.	

3.	unincorporated association or body of individuals	beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to **more than 15 per cent** of the property or capital or Profits of the unincorporated association or body of individuals.
4.	Where no natural person is identified under (1), (2) or (3) above	Beneficial owner is the relevant natural person who holds the position ofsenior managing official.
5.	Trust	identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with **10% or more** interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
6.	Where the customer or the owner of the controlling interest is a company listedon a stock exchange, or isa subsidiary ofsuch a company,	it is not necessary to identify and verify the identity of any shareholder orbeneficial owner of such companies.

Annexure III – Characteristics of High Risk Customer and Medium Risk Customers
Characteristics of High Risk Customers

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such asUN 1267 etc.;
2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
3. Individuals and entities in watch lists issued by Interpol and other similar international organizations;
4. Customers with dubious reputation as per public information available or commercially availablewatch lists;
5. Individuals and entities specifically identified by regulators, FIU and other competent authoritiesas high-risk;

6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;
7. Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
8. Non face-to-face customers;
9. High net worth individuals;
10. Firms with 'sleeping partners' ;
11. Companies having close family shareholding or beneficial ownership ;
12. Complex business ownership structures, which can make it easier to conceal underlyingbeneficiaries, where there is no legitimate commercial rationale;
13. Shell companies which have no physical presence in branch locations. The existence simply of alocal agent or low level staff does not constitute physical presence;
14. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clientswhere the identity of the underlying client is not disclosed to the NBFC;
15. Client Accounts managed by professional service providers such as law firms, accountants, agents,brokers, fund managers, trustees, custodians, etc;
16. Trusts, charities, NGOs/ unregulated clubs and organizations receiving
17. donations;
18. Gambling/gaming including “Junket Operators” arranging gambling tours;
19. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art andantique dealers and auction houses, estate agents and real estate brokers);
20. Customers engaged in a business which is associated with higher levels of corruption (e.g., armsmanufacturers, dealers and intermediaries;
21. Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
22. Customers that may appear to be Multi-level marketing companies etc.

Characteristics of Medium Risk Customers

1. Stock brokerage;
2. Import / Export;
3. Gas Station;
4. Car / Boat / Plane Dealership;
5. Electronics (wholesale);
6. Travel agency;
7. Telemarketers; Providers of telecommunications service, internet café, IDD call service, phone

Annexure IV – Standards with respect to undertaking Video – Customer Identification Process(V-CIP)

1. **V-CIP Infrastructure**

a. The Company shall comply with the RBI guidelines on minimum baseline cyber security andresilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure shall be housed in the Company's own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the company only and all the data including video recording is transferred to the company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the company.
b. The Company shall ensure end-to-end encryption of data between customer device and thehosting point of the V-CIP application, as per appropriate encryption standards. The customer consent shall be recorded in an auditable and alteration proof manner.
c. The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
d. The video recordings shall contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall beadequate to allow identification of the customer beyond doubt.
e. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification shall rest with the Company. Appropriate artificial intelligence (AI) technology may be used to ensure that the V-CIP is robust.
f. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as acyber security event under extant regulatory guidelines.
g. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / Regulatory guidelines.
h. The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

2. V-CIP Procedure

a. The Company shall formulate a clear work flow and standard operating procedure for V-CIPand ensure adherence to it. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official shall be capable to carry out livenesscheck and detect any other fraudulent manipulation or

suspicious conduct of the customer and act upon it.

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

c. The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

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

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

f. The authorized official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
   i. OTP based Aadhaar e-KYC authentication
   ii. Offline Verification of Aadhaar for identification
   iii. KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer
   iv. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker

g. The Company shall ensure to redact or blackout the Aadhaar number as per the relevant regulatory guidelines.

h. 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 working days from the date of carrying out V-CIP.

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

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

k. The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through DigiLocker.

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

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

n. Assisted V-CIP shall be permissible when the Company takes help of Banking Correspondents (BCs) facilitating the process only at the customer end. The Company shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the Company.

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

p. All matters as required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

3. V-CIP Records and Data Management

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

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