INFINITY™
FINCORP SOLUTIONS
SANKALP AAPKA, SAATH HUMARA

INFINITY FINCORP SOLUTIONS PRIVATE LIMITED (IFSPL)

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

Reviewing Authority	Compliance Department
Approving Authority:	Board of Directors of Infinity Fincorp Solutions Private Limited
Date of Approval/Modification:	11.10.2025
Version No.:	V2
Context:	The policy is formulated pursuant to the following Regulatory Guidelines/ Notifications/ Circulars • RBI Master Direction on KYC, 2016 (DBR.AML.BC.No.81/14.01.001/2015-16) • Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023 ; • Prevention of Money Laundering Act, 2002 (PMLA) and related Rules

Preamble:

This Policy is framed in accordance with:

- RBI Master Direction on KYC, 2016 (DBR.AML.BC.No.81/14.01.001/2015-16)
- Prevention of Money Laundering Act, 2002 (PMLA) and related Rules

IFSPL is committed to preventing its operations from being used for money laundering or terrorist financing and ensures compliance through robust KYC and AML measures.

Background :

Money laundering refers to concealing or disguising the origin and ownership of the proceeds from criminal activity, including drug trafficking, public corruption, terrorism, fraud, human trafficking, and organized crime activities. Terrorist financing is the use of legally or illegally obtained funds to facilitate terrorist activities. Money laundering and terrorist financing may involve a wide variety of financial products, services, and transactions including lending and investment products, and the financing of equipment and other property that could be used to facilitate terrorism and other criminal activity.

Generally, the money laundering process involves three (3) stages: placement, layering and integration. As illegal funds move from the placement stage through the integration stage, they become increasingly harder to detect and trace back to the illegal source.

1. *Placement* is the point where illegal funds first enter the financial system.

2. *Layering* After illegal funds have entered the financial system, layers are created by closing and opening accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.

3. *Integration* occurs when the criminal believes that there are sufficient number of layers hiding the origin of the illegal funds to safely invest the funds or apply them towards purchasing valuable property in the legitimate economy.

To prevent money-laundering in India and to provide for confiscation of property derived from, or involved in, money-laundering and related matters, the Parliament of India enacted the Prevention of Money Laundering Act, 2002 (PMLA), as amended from time to time. Further, necessary Notifications / Rules under the said Act have been published and amended by the Ministry of Finance, the Government of India.

As per the Prevention of Money Laundering Act 2002, the offence of Money Laundering is defined as: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering. "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property." The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime. The Reserve Bank of India (RBI) vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, and subsequent modifications thereof, have prescribed guidelines "Anti Money Laundering" guidelines/ standards. In view of the above, AML - KYC policy of IFSPL has been framed to broadly achieve the following purposes:

a) To prevent criminal elements from using IFSPL for money laundering activities

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

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

d) To comply with applicable laws and regulatory guidelines.

e) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

This Policy will be applicable to all branches/offices/ Employees and agents/ representatives of IFSPL and is to be read in conjunction with related operational guidelines issued from time to time. It shall be effective from the date of approval of this policy and shall be reviewed as and when required by under the applicable rules and regulations.

The Risk Management Committee (RMC) will monitor and supervise implementation of the Policy. Further, any changes in the Policy shall be approved by the Board of Directors or the Risk Management Committee of the Company.

THE KEY ELEMENTS OF THE KYC AND AML POLICY ARE:

a. Customer Acceptance Policy (CAP);

b. Risk Management;

c. Customer Identification Procedures (CIP);

d. Monitoring of transactions

DEFINITIONS:

1. **Customer**

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.

2 Beneficial Owner:

1. Where the customer is a Company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.

   Explanation - 1. "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company. 2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

2. Where the customer is a Partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership.

3. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
   Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

4. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

3. Customer Due Diligence (CDD)

Identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

4.Officially valid document (OVD)

Officially Valid Document" (OVD) means the passport, the driving licence,proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. 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 PSUs, if they contain address.
iv. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation;

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

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.

5. **Person - means 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).

6. Senior Management - for the purpose of KYC compliance shall include Designated Director, Head of Credit, Head of Risk, Business Heads, Key Managerial Persons, Compliance Officer, Principal Officer (PO) and his/her supervisor.

CUSTOMER ACCEPTANCE POLICY ("CAP")

IFSPL's Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship with IFSPL broadly are detailed below:

a) No account is to be opened in anonymous or fictitious/benami name(s)/entity(ies).

b) No loan will be sanctioned/disbursed where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

c) Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a company desires to avail another loan with the Company, there shall be no need for a fresh CDD exercise.

d) Accept customers only after verifying their identity, as per CDD Procedures defined aforesaid and shall be followed for all the joint account holders (including guarantors) as well, while opening a joint account.

e) Necessary checks before opening a new account are to be ensured so 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. For this purpose, the Company shall maintain lists of individuals or entities issued by regulatory and enforcement agencies such as the RBI, United Nations Security Council (UNSC), and others, as well as internal lists the Company may decide from time to time. There are two types of lists maintained:
   i. Sanctions lists issued by regulatory authorities such as UNSC, RBI, OFAC, etc., which include individuals and entities subject to mandatory restrictions and prohibitions.
   ii. The Company's own Negative List, comprising individuals or entities identified internally as high-risk or prohibited based on the Company's policies and risk assessments.

   Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be treated as suspicious and reported.

f) Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorization.

g) Appropriate Enhanced Due Diligence (EDD) measures (refer Annexure I) shall be adopted for high risk customers from AML perspective, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically Exposed Persons (PEPs) and their family members/close relatives.

h) 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 (refer Annexure I) shall be adopted.

i) Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Prevention of Money Laundering Act, 2002 (PMLA) and RBI/ IFSPL guidelines/instructions are indicated in Annexure II to this Policy. The information collected from the Customers shall be kept confidential.

j) Not to open an account or close an existing account (except as provided in this Policy), where CDD measures as defined in this Policy could not be applied, due to non- cooperation of the customer or non-reliability of the data/ information furnished to IFSPL. Suitable built – in safeguards shall be provided to avoid any harassment to Customers.

k) Implementation of CAP should not become too restrictive and result in denial of IFSPL services to general public, especially to those who are financially or socially disadvantaged.

l) The decision to open an account for Politically Exposed Person (PEP) should be taken at a senior level. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

m) Circumstances, in which a customer is permitted to act on behalf of another person/ entity shall be clearly spelt out in conformity with the established law and practice and shall be strictly followed so as to avoid occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity or beneficial owner

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

o) Suitable system is put in place to ensure that the identity of the Customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India/Mentioned in the KYC Master Direction as updated from time to time.

p) IFSPL shall seek only such information from the customer which is relevant to the risk category and is not intrusive. Any other information from the customer should be sought separately with his/her consent and after opening the account.

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

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

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

s) Where RE 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.

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.

RISK MANAGEMENT

For Risk Management, the Company will have a risk based approach which includes the following:

i. Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the Company and as per the broad principles

ii. 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. 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.

iii. The customers will be monitored on regular basis with built in mechanism for tracking irregular behavior for risk management and suitable timely corrective action.

iv. The Company shall prepare a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy. The customer profile shall contain the information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by IFSPL. These requirements may be moderated according to the risk perception.

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

vi. The Company will not establish any business relationships with individuals and entities listed or identified in the United Nations Security Council (UNSC) Consolidated List, Office of Foreign Assets Control (OFAC) List, as well as watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high risks,etc. If any matches are found on the lists mentioned above, the company will not proceed to establish any business relationship with such party.

Company may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better. Company shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

The information collected from different categories of customers relating to the perceived risk shall be non-intrusive.

A. High Risk – (Category A):

High risk customers typically will include:

a. 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.;
b. Non - resident Customers (excluding applicants for retail education loans)
c. High net worth individuals without an occupation track record of more than 3 years
d. Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (Excluding applicants / beneficial owners who are running affiliated education institutions) – Refer Annexure I
e. Firms with sleeping partners
f. Politically exposed persons (PEPs) of Indian/ foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner h) Customers with dubious reputation as per public information available or commercially available watch lists.
g. Gambling/gaming including "Junket Operators" arranging gambling tours; j) Jewelers and Bullion Dealers; k) Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers); l) Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries; m)Customers that may appear to be Multi-level marketing companies etc. n) Any borrower/co-borrower working in a country identified as high risk.

A. Medium Risk – (Category B):

Medium risk customers typically will include:

a. Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (i.e. applicants / beneficial owners who are running affiliated education institutions)
b. Salaried applicant with variable income/ unstructured income receiving Salary in cheque
c. Salaried applicant working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialing (IDD) call service.
d. Self employed professionals other than HNIs (excluding applicants for retail education loans)
e. High net worth individuals with occupation track record of more than 3 years
f. One of more borrowers resident outside India (excluding student going abroad to study
g. Companies having close family shareholding or beneficial ownership. h) Non face to face to customers (Refer Annexure I)

B. Low Risk – (Category C):

Low risk customers typically will include:

a. Salaried employees with well defined salary structures
b. People working with government owned companies, regulators and statutory bodies etc.
c. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
d. People working with Public Sector Units
e. People working with reputed Public Limited Companies and Multinational Companies. All borrowers resident in India (including student going abroad to study)

f. Low risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other person not covered under above two categories.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP, the Company will obtain senior management approval in such cases to continue the business relationship with such person, and also undertake EDD measures as specified in Annexure I.

CUSTOMER IDENTIFICATION PROCEDURES ("CIP")

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

I. Commencement of an account-based relationship with the customer;
II. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained;
III. Selling their own products, selling third party products as agents and any other product for more than Rs.50,000/-.
IV. Carrying out transactions for a non-account based customer (walk-in customer);

The Company shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.

The Company will obtain Permanent account number (PAN) of customers as per the applicable provisions of Income Tax Rule 114B. Form 60 shall be obtained from persons who do not have PAN.

For the customers that are legal person or entities:

i. the Company will verify the legal status for the legal person/ entity through proper and relevant documents;

ii. the Company will understand the beneficial ownership and control structure of the customer and determine who the natural persons are and who ultimately controls the legal person.

Additional documentation may be obtained from the customers with higher risk perception as may be deemed fit. This shall be done having regard but not limited to location (registered office address, correspondence address and other addresses as may be applicable), nature of business activity, repayment mode & repayment track record.

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

i. Records or the information of such customers' due diligence carried out by the third party is immediately obtained by the Company or from the Central KYC Records Registry;

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

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

iv. The third party shall not be based in a country/ jurisdiction assessed as high risk;

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

While undertaking customer identification, the Company will ensure that:

i. Decision-making functions of determining compliance with KYC norms shall not be outsourced.

ii. The customers shall not be required to furnish an additional OVD, if the OVD submitted for KYC contains proof of identity as well as proof of address e.g. Passport.

iii. The customers will not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/ his local address on which all correspondence will be made by the Company. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as cheque books, ATM cards, telephonic conversation, positive address verification, Rent agreement, etc.

iv. In case of change in the address mentioned on the 'proof of address', fresh proof of address

should be obtained within a period of six (6) months.

v. Enhanced Due diligence measures are indicated in Annexure I. An indicative list of the nature and type of documents/information that may be relied upon for customer due diligence / identification is given in Annexure II.

Periodic Updating of KYC data: IFSPL 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 periodicity of updating of Customer's KYC data shall be once in 10 years for low risk customers, once in every 8 years for medium risk customers, and once in 2 years for high risk customers from the onboarding of customers /last kyc updation.**

I. <u>In case of Individual customers</u>

a) **where there is no change in KYC information**: a self-declaration from the customer in this regard shall be obtained through customer's registered email id or registered mobile number
b) **where there is change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's registered email-id or registered mobile number 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

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, if needed.

c) **Where the customers, who were minor at the time of opening account, attain majority:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Company. Wherever required, the Company may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

d) Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.
e) Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. 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.

II. **Customers other than individuals**

a) **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 through its registered email id, letter from an official authorized by the LE in this regard, board resolution etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available is accurate and shall update the same, if required, to keep it as up-to-date as possible.
b) **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.

The Company shall ensure that all the KYC documents as required under CDD is available with them. In case, wherever the KYC document has been expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that of on-boarding a customer.

The company shall ensure that PAN details are verified from the database of the issuing authority at the time of periodic updation of KYC and 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 mentioning the date of updation of KYC details, is provided to the customer.

CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

1. CDD Procedure in case of Individuals - The Company will obtain the following documents from an individual while establishing an account based relationship:

i. One (1) certified copy of an OVD as defined above containing details of identity and address (as per Annexure II);

ii. One (1) recent photograph; and

iii.Such other documents pertaining to the nature of business or financial status specified by the Company.

2. 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 cross selling or other purpose, except with the express consent from the customer.

3. Submission of PAN or form 60 in lieu of PAN and Aadhaar is mandatory for all customers, to the extent applicable, unless it is specifically exempted under any law/act/regulations/notification / circular etc.

Note: The Company will capture the KYC information for sharing with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, under the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company will

upload the KYC data pertaining to all types of prescribed accounts with CKYCR, as and when required, in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

4. The Company may print/download directly, the prospective customer's e-Aadhaar letter from the UIDAI portal, if such a customer knows only his/her Aadhaar number or if the customer carries only a copy of Aadhaar downloaded from a place/source elsewhere, provided, the prospective customer is physically present in the branch of the Company.

5. A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

6. If a person who proposes to open an account does not have an OVD as 'proof of address', such person shall provide OVD of the relative, with whom the person is staying, as the 'proof of address'. 'Relative' as per Section 2(77) of the Companies Act, 2013 shall mean and include:

i. Members of Hindu Undivided family (HUF),
ii. Husband or Wife,
iii. Father (includes step-father),
iv. Mother (includes step-mother),
vii. Brother (includes step-brother),
viii. Sister (includes step-sister),
ix. Son (includes step-son),
x. Son's wife,
xi. Daughter, and
xii. Daughter's husband

A declaration from the relative that the said person is a relative and is staying with him/her shall be obtained.

7. If a customer categorized as 'low risk' expresses inability to complete the documentation requirements on account of any genuine reason, and where it is essential not to interrupt the normal conduct of business, the Company may, at its discretion, complete the verification of identity of the customer within a period of 6 months from the date of establishment of the relationship.

Monitoring of Transactions:

Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. IFSPL shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. IFSPL may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve cash over and above Rs. 1 lac should particularly attract the attention of IFSPL. Higher risk accounts shall be subjected to intense monitoring.

IFSPL shall set key indicators for such accounts basis the background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring. IFSPL shall carry out the periodic review of risk categorization of transactions/customer's accounts and the need for applying enhanced due diligence measures at a periodicity of not less than once in six (6) months. IFSPL shall explore the possibility of validating the new account opening applications with various watch lists available in public domain, including RBI watch list.

Training Programme

IFSPL shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for frontline staff, compliance staff and officer/ staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

Internal Control System

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. 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 lapses observed in this regard. The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

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.

On-going employee training program will be put in place so that the members of staff are adequately trained in KYC & AML policy.

The concerned department would also ensure daily verification of lists: (i) of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council, and (ii) as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, for the purpose of taking into account any modifications to such lists in terms of additions, deletions or other changes.

Record keeping

a) Maintenance of records of transactions

The Company shall maintain proper record of the transactions as required under Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) read with Rules 3 of the PML Rules as mentioned below:

(i) All cash transactions of the value of more than Rs. 2 lacs, though by policy the Company does not accept cash deposits in foreign currency.
(ii) All series of cash transactions integrally connected to each other which have been valued below Rs. 2 lacs where such series of transactions have taken place within a month.
(iii) All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent 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;

(iv) records pertaining to identification of the customer and his/her address; and (vi) 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. An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure III.

b) Records to contain the specified information

The Records referred to above in Rule 3 of PMLA Rules to 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

Section 12 of PMLA requires the Company to maintain records as under: i. records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of five (5) years from the date of transactions between the clients and IFSPL. ii. records of the identity of all clients of IFSPL is required to be maintained for a period of five years from the date of cessation of transactions between the clients and IFSPL. IFSPL shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

The Company shall ensure that in case of customers who are non-profit organizations, 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. and maintain such registration records for a period of five years after the business relationship between the customer and the RE has ended or the account has been closed, whichever is later.

Appointment of Principal Officer

IFSPL shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Head/Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND and RBI.

Reporting to Financial Intelligence Unit - India

In accordance with the requirements under PMLA, the Principal Officer of IFSPL 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 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 endeavor to put in place automated systems for monitoring 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. An indicative list of suspicious transactions is enclosed as Annexure III.

The employees of IFSPL shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

Appointment of Designated Director

The Board of Directors shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. The "Designated Director" can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the "Designated Director". The name, designation and address of the Designated Director shall be communicated to the FIU-IND and RBI.

General

1. Closure of Accounts/Termination of Financing/Business Relationship

Where IFSPL is unable to apply appropriate KYC measures due to non furnishing of information and/or non-cooperation by the customer, IFSPL shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Chairman & Managing Director or key managerial persons authorized for the purpose.

2. KYC for the Existing Accounts:

While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions with existing customers would be continuously monitored for any unusual pattern in the operation of the accounts. 3. Updation in KYC Policy of Company

Principal Officer after taking the due approval from the Board of Directors of IFSPL shall make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.

Annexure I

Enhanced Due Diligence (EDD) measures

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

i. Branch/office shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

ii. Branch/office shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a Customer.

iii. The decision to provide financial services to an account for PEP shall be taken at a senior level and shall be subjected to monitoring on an ongoing basis.

iv. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

2. Accounts of non-face-to-face customers

2.1 In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk. Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes 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.

Following EDD measures shall be undertaken by the Company for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

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

ii) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.

iii) Apart from obtaining the current address proof, 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.

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

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

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

2.2 Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. 2.3 In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the NBFCs may have to rely on third party certification/ introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

3. Trust/Nominee or Fiduciary Accounts Branch/offices shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. IFSPL shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person

settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', branches shall take steps to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures

4. Accounts of companies and firms

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

Annexure II Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers

Money Laundering and Terrorist Financing Risk Assessment:

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

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

The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Risk Management Committee of the Company. However, it should be reviewed at least annually.

The outcome/update of the exercise shall be put up to the Risk Management Committee (RMC) and will be available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks. The Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Company shall monitor the implementation of the controls and enhance them if necessary.

INDIVIDUALS	A. KYC Identifier with an explicit consent to download records from CKYCR. 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 – o there is a change in the information of the customer as existing in the records of CKYCR;

	○ the current address of the customer is required to be verified; ○ the Company 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; ○ the validity period of documents downloaded from CKYCR has lapsed. or B. the proof of possession of Aadhaar number where offline verification can be carried out; and PAN OR FORM 60 or C. the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e- document thereof containing the details of his identity and address; and · PAN OR FORM 60 and · an equivalent e-document of any OVD or · certified copy of OVD ▪ Where the OVD furnished buy the customer does not have updated address, the following document shall be deemed to be OVDs for limited purposes of proof of address: ▪ Utility bills not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill) ▪ Property or Municipal Tax receipt ▪ Pension or Family pension payment orders ▪ 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. ▪ the customer shall submit OVD with current address within a period of three months of submitting the documents specified above. ▪ The company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means. Other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company.
PROPRIETORSHIP FIRM	❖ KYC for Individual as stated above AND ❖ Any two of the following as business proof in the name of the proprietary firm ○ Registration certificate (including "Udyam Registration Certificate (URC) issued by the Government") ○ Shop & Establishment Act documents ○ Sales & Income Tax returns ○ CST/VAT/GST Certificate ○ Sales Tax/Service Tax/Professional Tax Registration documents ○ Import/Export Code/License/Certificate of Practice issued in the name of proprietary concern by the professional body incorporated under statute. ○ Complete income tax returns (Not just acknowledgement) in the name of Sole Proprietor where the Firm's income is reflected/duly authenticated/acknowledged by IT ○ Electricity/Water/Landline Bills etc.

	However, in cases where the Company is satisfied that, for any proposal, the proprietary concern is not possible to furnish two such documents, the Company will have the discretion to accept only one of those documents as activity proof. In such cases, the Company, however, will undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.
PRIVATE / PUBLIC LIMITED COMPANY / LLPS	Certified copies each of the following documents or the equivalent e- documents • Certificate of Incorporation • Memorandum of Association & Articles of Association • Permanent Account Number of the company • Board Resolution • the names of the relevant persons holding senior management position • the registered office and the principal place of its business, if it is different • KYC as per KYC norms for individual relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
PARTNERSHIP FIRM	Certified copies each of the following documents or the equivalent e-documents • Registration Certificate • Partnership Deed • Permanent Account Number of the partnership firm • the names of all the partners and • address of the registered office, and the principal place of its business, if it is different. KYC as per KYC norms for individual relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the firm's behalf.
TRUST	Certified copies each of the following documents or the equivalent e-documents • Registration Certificate • Trust Deed • Permanent Account Number or Form No.60 of the trust • KYC as per KYC norms for individual relating to beneficial owner, managers, officers or employees, as the case may be, holding a power of attorney to transact on its behalf, for those discharging role as trustee and authorized to transact on behalf of the trust • the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust • the address of the registered office of the trust; List of trustees
Unincorporated associations 1. Association of Persons (AOP) 2 . B o d y o f Individuals (BOI) Explanation 1: Unregistered trusts/ partnership firms shall be included under the term 'unincorporated association'.	Certified copies each of the following documents or the equivalent e-documents · Resolution of Society/Firm · Power of Attorney (PoA) in this regard · Permanent Account Number or Form No.60 · KYC as per KYC norms for individual relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney on it's behalf. Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.

Explanation 2: Term 'body of individuals' i n c l u d e s societies.	
J u r i d i c a l persons not specifically covered in the earlier part, such as Government o r i t s Departments, S o c i e t i e s , Universities and Local bodies like V i l l a g e Panchayats	Certified copies each of the following documents or the equivalent e-documents · Document showing name of the person authorized to act on behalf of the entity · KYC as per KYC norms for individual relating to person holding an attorney to transact on it's behalf. Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals

In case any document not part of this list is submitted by the Customer, the same shall be with explicit consent of the Customer.

Annexure III

A. Broad categories of reason for suspicion and examples of suspicious transactions for Non Banking Financial Companies are indicated as under: Identity of client - False identification documents - Identification documents which could not be verified within reasonable time - Accounts opened with names very close to other established business entities Background of client - Suspicious background or links with known criminals Multiple accounts - Large number of accounts having a common account holder, introducer or authorized signatory with no rationale Activity in accounts - Unusual activity compared with past transactions Nature of transactions - Unusual or unjustified complexity - Involves proceeds of an criminal / illegal

activity, regardless of the value involved - No economic rationale or bonafide purpose - Frequent purchases of drafts or other negotiable instruments with cash - Nature of transactions inconsistent with what would be expected from declared business - Reasonable ground of suspicion that it may involve financing of activities relating to terrorism and/or account holder / beneficial owner linked or related to terrorist, terrorist organization or those who finance or attempt to finance terrorist activities. Value of transactions - Value just under the reporting threshold amount in an apparent attempt to avoid reporting - Value inconsistent with the client's apparent financial standing.

B. Illustrative list of Suspicious Transactions

- Reluctant to part with information, data and documents
- Submission of false documents, purpose of loan and detail of accounts
- Reluctance to furnish details of source of funds of initial contribution
- Reluctance to meet in person, representing through power of attorney
- Approaching a distant branch away from own address
- Maintaining multiple accounts without explanation
- Payment of initial contribution through unrelated third party account
- Suggesting dubious means for sanction of loan
- Where transactions do not make economic sense
- Where doubt about beneficial ownership
- Encashment of loan through a fictitious bank account
- Sale consideration quoted higher or lower than prevailing area prices
- Request for payment in favor of third party with no relation to transaction
- Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent
- Frequent request for change of address
- Overpayment of installments with a request to refund the overpaid amount
- Approvals/sanctions from authorities are proved to be fake
- Overpayment of installments with a request to refund the overpaid amount

Modified and Reviewed by		Approved by
Kamlesh Shah	Shankar Masale	Shrikant Ravalkar