Nilfee Anti-Money Laundering Policy Statement & Evaluation Procedures

Compliance and Supervisory Procedures

for Nilfee Fintech Private Limited

No 2/21, Sabari Bahavan Flats, Vijay Avenue Third Street, Naganallur, Chennai- 600061

https://nilfee.com/ | https://usdcinr.com

Registered under FIU-IND (REID VA00002375)

Revised by D. Lakshmi Priya dated 01/04/2024

Company Anti-Money Laundering Policy Statement

Nilfee Fintech Private Limited has a strict policy against and actively works to prevent money laundering, as well as any activities that aid money laundering, terrorism financing, or criminal endeavors.

Money laundering is broadly described as participating in actions designed to hide or alter the true source of unlawfully acquired proceeds, making them appear to come from legitimate sources or constitute lawful assets. Typically, money laundering unfolds in three phases:

- **Placement:** Illicitly generated cash is converted into monetary instruments like money orders or traveler's checks, digital money, crypto assets, or it is deposited into financial institution accounts.

- **Layering:** Funds are moved or transferred to other accounts or financial institutions, enhancing the separation between the money and its criminal origins.

- **Integration:** Funds are reintroduced into the economic system, used to acquire lawful assets, or employed to finance other criminal activities or legitimate businesses. While terrorist financing may not always involve the proceeds of criminal activities, it often entails attempts to conceal the funds' origin or intended use, which will later be directed toward criminal purposes.

The Government of India has serious concerns over money laundering activities which are not only illegal but anti-national as well. Money laundering is the process by which large amount of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from a legitimate source. All crimes that produce a financial benefit give rise to money laundering.

The Prevention of Money Laundering Act, 2002 has come into effect from 01st July, 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 01st July, 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

As per the provisions of the PMLA, every banking company, financial institution (which includes a chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with the digital assets shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- All cash transactions of the value of more than Rs. 10 lakh (Rupees Ten Lakh) or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lakh (Rupees Ten Lakh) or its equivalent in foreign currency where such series of

transactions have taken place within a month and the monthly aggregate exceeds an amount of Rs. 10 lakh (Rupees Ten Lakh) or its equivalent in foreign currency.

- All suspicious transactions whether or not made in cash and including, inter- alia, credits or debits into from any non-monetary account such as demat account, security account maintained by the registered intermediary.

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.

The Anti - Money Laundering Guidelines provide a general background on the subject of money laundering and terrorist financing in India and provides guidance on the practical implications of the PMLA. The PMLA Guidelines sets out the steps that a registered intermediary and any of its representatives, need to implement to discourage and identify any money laundering or terrorist financing activities.

Financial Intelligence Unit (FIU) – INDIA

The Government of India has set up Financial Intelligence Unit-India (FIU-INDIA) on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the finance minister.

FIU–INDIA has been established as the central national agency responsible for receiving, processing, analysing, and disseminating information relating to suspect financial transactions. FIU-INDIA is also responsible for coordination and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

OBJECTIVES OF THESE GUIDELINES OBJECTIVES OF THESE GUIDELINES

The purpose of this Policy is to guide all the employees of Nilfee Fintech Private Limited and employees of its associates on the steps that they are required to take and implement to prevent and identify any money laundering or terrorist financing activities. It shall be the responsibility of each of the concerned employees that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and requirements as enshrined in the "Prevention of Money Laundering Act, 2002".

Accordingly, the Company has laid down following policy guidelines:

Principal Officer:

Director of the company is appointed as the Principal Officer. He will be responsible for implementation of internal controls & procedures for identifying and reporting any suspicious transaction or activity to the concerned authorities. Principle officer has the right of timely access to customer identification data, other CDD information and is able to report the same to senior management or the board of directors.

Designated Director:

Mr. L. Lalithbabu is appointed as the Designated Director of the company in terms of rule 2 (ba) of the PML rules.

In terms of section 13 (2) of PML Act (as amended by the Prevention of Money-laundering (Amendment) Act, 2012), the Director, FIU-IND can take appropriate action, including levying monetary penalty, on the designated director for failure of the intermediately to comply with any of its AML/CFT obligation.

OBLIGATION TO ESTABLISH POLICIES AND PROCEDURES

- Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including Virtual Asset Service Provider (VASP), to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all intermediaries ensure the fulfilment of the aforementioned obligations.
- To be in compliance with these obligations, the senior management of a registered VASP is fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. Accordingly, Nilfee Fintech Private Limited should:

  1. issue a statement of policies and procedures, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
  2. ensure that the content of these Directives are understood by all staff members;
  3. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;
  4. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
  5. undertake client due diligence ("CDD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

Policies and procedures to combat ML shall cover:

- ✓ Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handles account information, securities transactions, money, and client records etc. whether in branches, departments, or subsidiaries;
- ✓ Client acceptance policy and client due diligence measures, including requirements for proper identification;
- ✓ Maintenance of records;
- ✓ Compliance with relevant statutory and regulatory requirements;
- ✓ Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
- ✓ Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating, and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front-line staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately

resourced, and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

Written Anti Money Laundering Procedures:

Nilfee Fintech Private Limited have adopted written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures should include client due diligence process covering:

- ✓ policy for acceptance of clients;
- ✓ procedures for identifying the clients; and
- ✓ transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

IMPLEMENTATION OF PMLA POLICY

1) Policy objectives

- To prevent criminal elements from using our business for money laundering activities or the funding of terrorist or criminal activities;
- To understand the customers and their financial dealings better, which in turn would help us manage the risk prudently;
- To put in place appropriate controls for detecting and reporting suspicious transactions in accordance with the applicable laws/ procedures laid down;
- To comply with applicable laws and regulatory guidelines; and
- To comply with PMLA Act, Rules and amendments issued from time to time.

2) Scope

These policies and procedures will apply to the operation of the Company in respect of businesses undertaken by it in its capacity of an VASP Registered under **FIU-IND (REID VA00002375)** and are to be read in conjunction with the existing guidelines.

3) Key Elements of the Policy

3.1 No cash transactions

The Company will not enter into any cash transactions with its clients for any reason whatsoever.

3.2 Customer Due Diligence process

FIU-IND from time to time has issued various amendments and circulars/guidelines specifying the documents required to be verified and submitted for opening of accounts of the clients in respect of **VASP** operations.

In short, while opening accounts of individuals, the original documents relating to proof of identity, proof of residence, PAN card are obtained and verified by an official of the Company.

Moreover 'in person verification' of the client is carried out by the officials of the Company and this fact is recorded in the application form. While opening of accounts in respect of entities other than individuals- documents like Memorandum of Association, Articles of Association, Board Resolution, photographs of authorized signatories, etc. are obtained.

In addition to this, PAN card details are verified on the Income Tax website. Websites of SEBI (www.sebi.gov.in) and Watch out Investors (www.watchoutinvestors.com) are also checked, to verify whether the person/entity is prohibited from trading in securities.

3.2.1. The CDD measures comprise the following

- Obtaining sufficient information in order to identify persons who beneficially own or control the Nilfee account. Whenever it is apparent that the digital assets acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;
- Verify the client's identity using reliable, independent source documents, data, or information;
- Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted-

I. For clients other than individuals or trusts: Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

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

Explanation: Controlling ownership interest means ownership of/entitlement to:

- more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
- more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

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

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

II. For client which is a trust: Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

III. The **VASP** shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits.

- Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (3);
- Understand the ownership and control structure of the client;
- Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and
- Nilfee Fintech Private Limited shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

3.2.2. Customer Acceptance Policy

3.2.2.1 Identification of the types of clients that are likely to pose a higher-than-average risk of money laundering or terrorist financing so that Nilfee Fintech Private Limited is in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. The following safeguards are to be followed while accepting the clients:

a) No account to be opened in a fictitious / benami name or on an anonymous basis.

b) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined inter alia having regard to clients' location, nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters should enable classification of clients into low, medium, and high risk. Clients will be categorised into low, medium, and high-risk clients enabling proper monitoring and risk management. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.

c) Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirements **FIU–IND.**

d) No account is opened where we are unable to apply appropriate CDD measures/ KYC policies or the information provided is suspected to be non-genuine, or if there is perceived non-cooperation of the client in providing full and complete information.

e) The circumstances under which the client is permitted to act on behalf of another person/entity should be clearly laid down. It should be specified in what manner the account should be operated, transaction limits for operation, additional authority required for transactions exceeding a

specified quantity / value and other appropriate details. The rights and responsibilities of both the persons i.e., the agent – client registered with the intermediary, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client should also be carried out.

f) Necessary checks and balances to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

g) The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

h) All Clients during on-boarding are screened against our internal system wherein, any client falling in SEBI Debarred, UNSC Sanctions List and UAPA orders are flagged off and restricted from account opening. Further, checks are in place and screening is done for FATF Public statements published/advised by the SEBI. These need to be reviewed & checked as per the orders/guidelines published by the regulators to identify whether any client is forming a part of that list, in that case such clients shall be blocked and reported to regulatory agencies accordingly.

3.2.3. Risk-based Approach and Risk Profiling of the Client

a) The Company should accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher-than-average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as low risk, medium risk and high-risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high-risk client(s), we have to apply a higher degree of due diligence. The factors of risk perception depend on client's KYC details, location, nature of business/trading activity, turnover, nature of transaction, and manner of payment etc.

In order to achieve this objective, all the clients should be classified in the following category:

Category A – Low Risk;

Category B – Medium Risk; and

Category C – High risk.

High Risk: Clients of special category (CSC) are considered as high-risk client such as:

i. Non-resident clients;
ii. High net worth clients;
iii. Trust, Charities, NGOs and organizations receiving donations;
iv. Companies having close family shareholdings or beneficial ownership;
v. Politically Exposed Persons (PEP) 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.

vi. Clients in high-risk countries. While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, intermediaries apart from being guided by the Financial Action task Force (FATF) statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude intermediaries from entering into legitimate transactions with clients from or situate in such high-risk countries and geographic areas or delivery of services through such high-risk countries or geographic areas;

vii. Non face to face clients;

viii. Clients with dubious reputation as per public information available etc.

The above-mentioned list is only illustrative, and Nilfee Fintech Private Limited at its discretion can classify any other set of clients in the high-risk category. Accounts which belong to the "Clients of Special Category" will be flagged and precaution will be taken with respect to their operation.

Medium Risk: The following clients are considered as medium risk:

i. Individuals with occupation such as business and agriculture;

ii. Legal entities like body corporate, partnership firms, LLP, HUF and etc.

Low Risk: Clients which do not fall under high risk/medium risk category get classified under low risk.

b) Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

c) The Company will be careful while monitoring the transactions of B and C Category clients. Where a client is classified under Medium or High-Risk Category, the said accounts should be kept under the supervision of a Principal Officer and an appropriate action should be taken as and when required.

d) Apart from this, the Company needs to exercise extra caution while monitoring the transactions of NRI/NRE/PIO and foreign clients, especially when the payment is being made in foreign currency.

e) In case of any change in the risk profile of the client, the same is modified in our system as per the risk category defined above.

3.2.4. Risk Assessment

a) Nilfee Fintech Private Limited shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to:

- Clients,
- Countries or geographical areas,
- Payment methods used by clients,
- Nature and volume of transactions,
- large number of accounts having a common account holder,
- Unexplained transfers between multiple accounts with no rationale,
- Unusual activity compared to past transactions,
- Doubt over the real beneficiary of the account,
- Pay-out/pay-in of funds and digital assets transferred to / from a third party, and
- Large sums being transferred from overseas for making payments.

The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, reference shall be made to the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions which shall be accessed from: http://www.un.org

b) The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk, the appropriate level, and the type of mitigation to be applied. The assessment shall be documented, updated regularly, and made available to competent authorities and self- regulating bodies as and when required.

c) A thorough assessment should be carried out to ascertain whether the client is dealing with us on his own behalf or someone else is the beneficial owner. If there are doubts, before acceptance of the clients, thorough due diligence should be carried out to establish the genuineness of the claims of the clients. Secrecy laws shall not be allowed as a reason for refusal to disclose the true identity of the client.

d) A detailed search should be carried out to ensure that the Client is not in defaulters/negative list of regulators. (search shall invariably be carried out on SEBI website www.sebi.gov.in, Ministry of Corporate Affairs sponsored website www.watchoutinvestors.com and UN website at http://www.un.org)

3.2.5. Client Identification Procedure

I. The KYC policy shall clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

We shall be in compliance with the following requirements while putting in place a Client Identification Procedure (CIP):

a) We shall proactively put in place appropriate risk management systems to determine whether our client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs. Further, the enhanced CDD measures shall also be applicable where the beneficial owner of a client is a PEP.

b) Employees are required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, we shall obtain senior management approval to continue the business relationship.

c) We shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

d) The client shall be identified by using reliable sources including documents / information. We shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

e) The information must be adequate enough to satisfy the competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by our Company in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.

f) Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within our Company.

3.2.6. Reliance on third party for carrying out Client Due Diligence (CDD)

1) Nilfee Fintech Private Limited may rely on a third party for the purpose of:

(a) identification and verification of the identity of a client; and

(b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PMLA.

2) Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by regulatory body from time to time. Further, the Company shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

3.3 Record Keeping

a) Nilfee Fintech Private Limited shall ensure compliance with the record keeping requirements contained in the **FIU-IND**, Rules and Regulations made there-under, PMLA as well as other relevant Legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

b) Nilfee Fintech Private Limited shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

c) Should there be any suspected drug related to laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, we shall retain the following information for the accounts of our clients in order to maintain a satisfactory audit trail:

i) the beneficial owner of the account;
ii) the volume of the funds flowing through the account; and
iii) for selected transactions:
- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

d) Nilfee Fintech Private Limited shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g., client identification, account files, and business correspondence, for periods which may exceed those required under the FIU-IND, Rules and Regulations framed there-under PMLA, other relevant Legislations, Rules and Regulations or Exchange Bye-laws or Circulars.

e) More specifically, Nilfee Fintech Private Limited has put in place a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules as mentioned below:

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

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

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

iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

3.4 Information to be maintained

Nilfee Fintech Private Limited shall maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

- the nature of the transactions;
- the amount of the transaction and the currency in which it is denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

3.5 Retention of Records

a) We have an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five (5) years from the date of transactions between the client Nilfee Fintech Private Limited.

b) As stated in sub-section 3.2.5, we implement the CIP requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five (5) years after the business relationship has ended or the account has been closed, whichever is later.

c) In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, we shall be retained until it is confirmed that the case has been closed.

e) **Records of information reported to the Director, Financial Intelligence Unit – India (FIU–IND):** We shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU–IND, as required under Rules 7 and 8 of the PML Rules, for a period of five (5) years from the date of the transaction between the client and Nilfee Fintech Private Limited.

4) Monitoring of Transactions

- Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that it can identify deviations in transactions / activities.
- Nilfee Fintech Private Limited shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The Company may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose

thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to FIU-IND and other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five (5) years from the date of transaction between the client and Nilfee Fintech Private Limited.

- Nilfee Fintech Private Limited shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the Company.
- Further, the compliance cell of Nilfee Fintech Private Limited shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.
- If any transaction appears to be suspicious, it is to be reported to the Compliance Department / Principal Officer & Designated Director immediately.
- For effective monitoring, internal alerts system is in place wherein alerts based on Red Flag Indicators (RFI) as mandated by FIU are generated by surveillance system. These alerts are analysed w.r.t the below points:

    - The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or documents.
    - The customer wishes to engage in a transaction that lack business sense or is inconsistent with the customer's stated business.
    - The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
    - Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
    - The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
    - The customer exhibits a lack of concern regarding transaction costs.
    - The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
    - The customer has difficulty describing the nature of his or her business.
    - The customer attempts to conduct frequent or large transactions, or asks for exemptions from the Company's AML policies.
    - The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the 10 Lakh government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
    - For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
- The customer has unexplained or sudden extensive money service activity, especially when they that had little or no previous activity.
- The customer has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer has financial activity with no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements.
- The customer uses multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent purpose.
- The customer has inflows of funds or other assets well beyond the known income or resources of the customer.

5. Suspicious Transaction Monitoring and Reporting

- Nilfee Fintech Private Limited shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.
- A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions, other facts and circumstances:

    1) Clients whose identity verification seems difficult or clients that appear not to cooperate;
    2) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
    3) Clients based in high-risk jurisdictions;
    4) Substantial increases in business without apparent cause;
    5) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
    6) Attempted transfer of investment proceeds to apparently unrelated third parties;
    7) Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export- import of small items

- Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer or any other designated officer within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Principal Officer/ Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.
- It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.
- FIU-IND categorizes clients of high-risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC'. Intermediaries are directed that such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.
- Nilfee Fintech Private Limited will, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

6) List of Designated Individuals/ Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at http://www.un.org. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

7) Procedure for freezing of funds, financial assets or economic resources or related services

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an amended Order dated February 2nd, 2021 detailing the procedure for the implementation of Section 51A of the UAPA.

8) Reporting to Financial Intelligence Unit-India

a) In terms of the PML Rules, intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address: **Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021. Website: http://fiuindia.gov.in**

b) We shall carefully go through all the reporting requirements and formats that are available on the website of FIU–IND under the Section Obligation of Reporting Entity – Furnishing Information – Reporting Format (https://fiuindia.gov.in/). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents While detailed instructions for filing all types of reports are given in the instructions part of the related formats, we shall adhere to the following:

i) The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

ii) The Suspicious Transaction Report (STR) shall be submitted within seven (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. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

iii) The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

iv) The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

v) Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.

vi) No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.

c) We shall not put any restrictions on operations in the accounts where an STR has been made. Our directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that an STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/or

related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

It is clarified that the registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

9) Employees' Hiring / Employees' Training / Customers' Education

a) Hiring Policy

Nilfee Fintech Private Limited follows high standards when hiring employees. We give preference to candidates referred by our existing employees, employees of group concerns:

➢ Interview by the HR;

➢ Interview by the head of the department which has requisitioned for filling vacancy;

➢ We do background check for employees with the help of information available on the internet, references given by candidates as well as independently through tie-ups with recruitment agency or third-party verification;

➢ No candidate is selected who has dubious character or there is negative information provided by his or her reference;

➢ As such the use of outside search firm is discouraged, but if required, we go for the same, to check whether we are able to get some good candidate(s) from it, but the procedure to be followed post selecting the candidate(s) remains the same. Our reference check is also there additional to recruitment agency.

After the selection, the candidate has to adhere to code of conduct as prescribed by Nilfee Fintech Limited from time to time.

b) Training

We have regular training programmes, where the staff members (front office, back office, compliance, risk etc.) are updated about the AML and CFT procedures. Adequate training should be given to all the concerned employees and clients to: i) ensure that the contents of the guidelines are understood; and ii) develop awareness and vigilance to guard against money laundering and terrorist financing.

c) Customers' Education

Implementation of AML/CFT measures requires intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regards to the motive and purpose of collecting such information.

There is, therefore, a need for Nilfee Fintech Private Limited to sensitize their clients about these requirements as the ones emanating from AML and CFT framework.

Accordingly, the above process is required and in place during monitoring of clients' transactions.

Nilfee Fintech Private Limited shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

10. Sanction Screening, Adverse Media, and PEP Check

A. Sanction Screening & PEP Check

As part of our customer due diligence (CDD), we partner with third party KYC/AML service providers like "PERSONA" (https://withpersona.com/) OR "ONFIDO" (https://onfido.com/) to screen our users on regular basis for sanction screening and PEP Checks. Nilfee will be screening for politically exposed persons (PEPs) and sanctions for ensuring that we never provide any of our services to companies or individuals liked directly or indirectly with the sanctioned individuals or companies.

A person could be a politically exposed person if they are:

- Heads of state or government, ministers or deputy/assistant ministers.
- Members of parliament or of similar legislative bodies (but not local government).
- Members of the governing bodies of political parties that are in power.
- Members of supreme courts, constitutional courts or any judicial body whose decisions are not subject to further appeal except in exceptional circumstances.
- Members of courts of auditors, or those on the boards of central banks.
- Ambassadors or senior members of the armed forces.
- Members of the administrative, management or supervisory bodies of state-owned enterprises.
- Directors, deputy directors, senior management, and members of the board of international organisations.
- If they have ceased to fulfil one or more of the public functions listed above within the last 12 months.
- People who are family members or close business associates of any of the above.

Part of this involves checking if they are on international blacklists or financial sanctions lists. If they are, or if we suspect illegal activity is taking place, we will refuse to work with the company or individual and submit a STR to the FIU-IND.

A. Real Time Screening for Adverse Media.

Nilfee customer due diligence includes real time identifying any publicly available information that may pose an impact. This includes relevant social media searches, news articles, ongoing or past legal or regulatory action, criminal history and much more. This information is available up-to-date and from a vast range of sources, making Adverse Media checks a vital step for our business looking to undertake widespread monitoring as part of our risk management strategy. We use above

mentioned (10.A) third party services to check and update our userbase with any new additions to the list. If found we will immediately block the user access and report to FIU-IND.

11. Bank / Company Relationship

We will work closely with our payment processor, BaaS provider, banking firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. The appropriate notification forms can be found at http://fiuindia.gov.in Generally we have agreed that the Company will monitor customer activity including proper customer identification information as required.

12. Program to Test AML Program

Annual testing of our AML program will be performed either by an independent third party which is primarily focused on PML Act compliance matters or other qualified independent third party or internally by a qualified member of the Company's staff. The annual testing will include an audit of our compliance with our AML program.

The auditor will issue a report of the auditor's findings upon completion their audit to senior management. We will address each of the resulting recommendations.

13. Monitoring Employee Conduct and Accounts

We will subject employee money service transactions to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Officer's accounts will be reviewed by a qualified member of the Company staff.

14. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to an appropriate member of senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them.

15. Additional Areas of Risk

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above and is continually working to improve its AML program.

16. Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor the Company's ongoing compliance with the requirements of the AML regulatory authority and the implementing regulations under it.

Signed: 

Name: Lalithbabu Logeshwarrao

Title: CEO