Kaleidofin Capital Private Limited	
Charter name	KYC and AML Policy
Version	1.0
Date of Board Approval	11 August 2022
Frequency of Review	As and when such review becomes necessary, on account of any changes in regulations or the business practices of the Company
Valid up to	Until reviewed by the Board

Kaleidofin Capital Private Limited

KYC and AML Policy

1. Purpose and Scope

1. The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

2. The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps Kaleidofin Capital Private Limited ("KCPL" or "the Company") to manage its risks prudently.

3. Accordingly, the main objective of this policy is to enable the Company to ensure proper identification of its customers.

4. This policy is applicable to all categories of products and services offered by the Company. The scope of the policy is:

    - To lay down explicit criteria for acceptance of customers.
    - To establish procedures to identify of individuals/non-individuals for opening of account.
    - To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
    - To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

    To fulfil the scope, the following four key elements will be incorporated into the Company's policy:

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

2. Compliance with the Policy

1. KCPL shall ensure that the compliance with this Policy is being checked in the internal process audits conducted on the Company.

2. The Company shall ensure that the decision-making functions are not outsourced.

3. All the procedures namely, Customer Due Diligence (CDD) procedure, risk management, customer identification process shall be carried out for all the business verticals of the Company.

3. Customer Acceptance Policy

Definition of a Customer:

- A person or entity that maintains an account and/or has a business relationship with the Company
- One on whose behalf the account is maintained (i.e. the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers.
- Chartered Accountants, Solicitors etc. as permitted under the law, and
- Any other person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of high value demand draft as a single transaction.

A "Person" shall have the meaning as defined under the Master Direction – Know Your Customer Direction, 2016 of RBI (and any amendment made thereto from time to time by RBI).

4. Guidelines for Accepting Customers

The following norms and procedures will be followed by the Company in relation to its customers who approach the Company for availing financial facilities:

1. No loan or other account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account.i.e. Benami Account. The Company shall insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.

2. No loan account or other will be opened where the company is unable to apply appropriate Customer Due Diligence measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

3. The Company shall not open any account or give / sanction any loan or close an existing account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:

    - The Company is unable to verify the identity of the customer
    - The customer without any valid or convincing reasons refuses to provide documents

to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity

- Information furnished by the customer does not originate from the reliable sources or appears to be doubtful due to lack of supporting evidence.
- Identity of the customer, directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.

4. Subject to the above-mentioned norms and caution, at the same time all the employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

5. The Operations Department shall, at the time of approving a financial transaction/activity, or executing any transaction, verify the record of identity, signature proof and proof of current address or addresses including permanent address of the customer. For co-lending and business correspondent partnerships, the KYC documents with Original Seen and Verified (OSV) confirmation shall be sent to the Company by the partner and the documents shall be further verified by the the Operations Department of the Company.

6. Suitable systems are 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.

7. Where an equivalent e-KYC document is obtained from the customer, the Company's partner and the Operations Department of the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and relevant regulations from the Reserve Bank of India in this regard.

5. Risk Level Categorization

1. The Company shall categorize its customers based on the risk perceived by the Company. The levels of categorization would be Low Risk, Medium Risk and High Risk. The risk categorization would be a function of different factors including the asset class, the industry the borrower operates in, the geography in which the borrower operates etc.

2. Special care and diligence will be taken and exercised in respect KYC verification of those customers who happen to be high profile and/or Politically Exposed Persons ("PEP") within or outside country. Such persons will include:

    - Foreign delegates or those working in Foreign high commissions or embassies,
    - Senior politicians,
    - Senior judicial officers,
    - Senior military officers,
    - Senior executives of state-owned corporations and
    - Officials of important and leading political parties (as explained in Master Direction - Know Your Customer (KYC) Direction, 2016).

3. Certain customers of special category (CSC) will also be subject to enhanced due diligence. An indicative and non-exhaustive list of such customers is as below:

    - NRI Customers
    - Trusts (except trusts appropriately set up under a specific regulation)
    - Societies
    - Charitable institutions
    - NGOs and other organizations receiving donations from within or outside the country
    - Partnership firms with sleeping partners
    - Family-owned companies
    - Persons with dubious or notorious reputation as per the information available from different sources like media, newspapers etc
    - Companies having close family shareholding or beneficial ownership
    - High net worth individuals
    - Non-face to face customers

6. Customer Data Confidentiality

For the purpose of preparing customer profile only such relevant information from the customers will be sought based on which the Company can easily decide about the risk category in which the customers are to be placed. Ordinarily, the customer profile maintained by the Company will be kept confidential except for cases where the customer himself allows and/or gives consent for the use of the information given in customer profile / application form for offering other products / services of other companies / entities belonging to the Company's group or any other legal entity with whom the Company is having any business tie-ups. However, while taking any such permission or consent of the customer for using his above referred information provided to the Company, it will be ensured that such permission / consent of the customer is unambiguous and explicit.

7. Customer Identification Procedure

The Company shall decide on 1) customer due diligence (CDD) procedures, 2) documents to be collected and stored and 3) KYC processes in accordance with the type of customer and nature of transaction / engagement / relationship with the Company. In accordance with regulations from the Reserve Bank of India in this regard, the customer identification procedure shall include:

- Establishing proof of identity (PoI)
- Establishing proof of address (PoA)
- Photograph (where applicable)
- Verification of business constitution documents (where applicable)
- Verification of business registration documents, including Goods and Services Tax registration, PAN card etc. (where applicable)
- RE-to-RE KYC
    - The Company may also rely on customer due diligence by third parties (subject to customer consent) that are Regulated Entities (REs) as defined by the Reserve Bank of India from time to time. In such cases, copies of the Officially Valid Documents (OVDs) shall be provided by the REs with Original Seen and Verified (OSV) certification from such REs and these documents shall be further verified by the

Operations Department of the Company. Alternatively, the Company may rely on Central KYC records as per information provided by the RE or the customer.

- Aadhaar-based e-KYC
    - The Company may carry out Aadhaar-based e-KYC, either with OTP authorization or with biometric authorization as per extant guidelines from the Reserve Bank of India and from the Unique Identification Authority of India (UIDAI)
    - This shall be subject to the Company receiving Aadhaar e-KYC Authentication Licence from UIDAI as applicable
- Video-KYC (in accordance with extant guidelines from RBI in this regard) (where applicable)

The Company shall not receive / rely on KYC documents for customers from its holding company.

Provisions under Prevention of Money Laundering Act (PMLA)

As per the provisions of Rule 9 of the Prevention of Money Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

- At the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship, and
- In all other cases, verify identify while carrying out:
    - Transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected,
    - Any international money transfer operations.

In terms of proviso to Rule 9 of the PML Rules, the relaxation, in verifying the identity of the client within a reasonable time after opening the account / execution of the transaction, stands withdrawn.
Abiding by the provisions of Rule 9, the Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The said Rule also require that the Company should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

Customer identification requirements shall be as per the provisions of the said rule.

8. Monitoring of Transactions and Maintenance of Transaction Records

1. The Company shall monitor transactions of a suspicious nature on an ongoing basis for the purpose of reporting it to the appropriate authorities. The extent of monitoring by the Company will depend on the risk sensitivity of the account and special attention will be given to all complex unusually large transactions, which have no apparent economic or lawful purpose. An illustrative (but not exhaustive) list of suspicious transactions is furnished in “Annexure 1”.

2. The Company shall exercise caution with respect to the transactions with persons (including

legal persons and other financial institutions) from the countries which have been identified by Financial Action Task Force (FATF) as high risk and non-cooperative jurisdictions with respect to compliance with the FATF Recommendations, 2012.

3. The Company shall file Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling under FATCA in terms of the direction of the RBI/PMLA in respect of all products/ services.

8.1 Ongoing due diligence

1. The Company shall undertake on going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and source of funds.

2. Any unusual pattern in the operations of the accounts like transaction exceeding threshold limits, high turnover in the accounts compared to the average outstanding etc shall be closely monitored. The extent of monitoring shall be aligned with the risk category of the Customer and high-risk category accounts shall be subjected to more intensified monitoring.

3. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

8.2 Periodic updation of KYC

1. As per the amendment to Master Direction on KYC dated 10th May 2021, the Company has adopted a risk-based approach for periodic updation of KYC in the following manner:

S. No.	Risk category	Frequency
1	**High risk customers**	Once in every two years from the date of opening of the account / last KYC updation
2	**Medium risk customers**	Once in every eight years from the date of opening of the account / last KYC updation
3	**Low risk customers**	Once in every ten years from the date of opening of the account / last KYC updation

2. The company shall obtain self-declaration from Individual customers and non- Individual customers in case of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained 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.

3. The Company shall obtain a copy of Officially Valid Documents (OVD) or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii) of Master Direction on KYC, for the purpose of proof of address, declared by the customer at the time of periodic updation.

4. In case of change in KYC information of non-individual customer, the Company shall undertake a KYC process which shall be equivalent to on-boarding a new customer.

8.3 Maintenance of Records of Transactions

The Company shall maintain proper records of the transactions as required under the

provisions of Prevention of Money Laundering Act (PMLA) and Rules. Specifically, the Company shall:

1. maintain all necessary records of transactions between itself and the customer for at least five years from the date of transaction or any other higher periods specified under law;

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

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

4. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

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

5. mantain a system for proper holding and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

9. Risk Management

1. The Company shall ensure that all departments work in co-ordination for implementation of the KYC policy. Heads of all the Departments will ensure that the respective responsibilities in relation to KYC policy are properly understood, given proper importance and appreciated and discharged with utmost care and attention by all the employees of the Company.

2. The Risk department of the Company will carry out periodic checks to determine as to whether all provisions of the KYC policy are being followed and adhered to by all the Departments concerned. The Audit Committee of the Board shall review adherence to the KYC guidelines at periodic intervals.

3. The Company's internal audit shall periodically evaluate the level of adherence to the KYC procedures. Audit function shall provide an independent evaluation of the effectiveness of

KYC policies and procedures, including legal and regulatory requirements.

4. High risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such high-risk accounts, based on factors mentioned under Section 5 of this policy document as well as the type of transactions involved (such as accounts having unusual transactions, inconsistent turnover, etc) and other risk factors.

10. General

10.1 Appointment of Designated Director

A 'Designated Director' means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board. (b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND and to the Reserve Bank of India as required by law. (c) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

10.2 Appointment of Principal Officer

To ensure effective implementation of this KYC Policy and a proper co-ordination and communication between the Company and RBI and other relevant enforcement authorities, the Company shall designate a senior official Principal Officer who will operate from the corporate office of the Company.

The name of the Principal Officer so designated, his designation and address including changes from time to time, shall be communicated to the Director, FIU-IND and to the Reserve Bank of India as required by law.

The Principal Officer shall be located at the Head / Corporate office of the Company. Mr Puneet Gupta, Chief Executive Officer has been appointed as the Principal Officer and the official responsible for ensuring fraud monitoring and reporting in accordance with Master Direction - Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016 dated September 29, 2016.

10.3 Reporting to Financial Intelligence Unit - India

The Principal Officer will report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director, FIU-IND,
Financial Intelligence Unit, India, 6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi - 110021

Where the Principal Officer has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of PMLA rules, such officer shall furnish information in respect of such transactions to the Director, FIU-IND, within the prescribed time.

A copy of all information furnished shall be retained by the Principal Officer for the purposes of official record.

10.4 Hiring of Employees and Training

The Company shall have adequate screening mechanism as an integral part of personnel recruitment / hiring process and also should have an ongoing employee training programs so that members of the staff having business and customer onboarding or risk management focused responsibilities are adequately trained in KYC/AML/CFT procedures. Training requirements shall have different focuses for front line staff and officer/staff dealing with new customers and managing relationship with existing customers, so that all concerned fully understand the rationale behind the KYC policies and implement them consistently.

10.5 Sharing KYC Information with Central KYC Records Registry

As per Paragraph 56 of Reserve Bank of India Master Direction DBR.AML.BC.No.81/14.01.001/2015 - 16 dated February 25, 2016, wherein all Regulated Entities (REs) have been advised to upload the KYC records pertaining to all new individual accounts opened on or after April 1, 2017 with Central KYC Records Registry (CKYCR) managed by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI). Accordingly, the Company shall capture the KYC information for uploading the data pertaining to all new individual accounts opened on or after 1/4/2017 with the CKYCR in accordance with the regulations in this regard.

Annexure 1

Illustrative list of Suspicious activities[1]

Transactions Involving Large Amounts of Cash

i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;

ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;

iii. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;

iv. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;

v. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;

vi. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchangeetc.;

vii. Depositing cash by means of numerous credit slips by a customer such that the amount of eachdeposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;

ii. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

ii. Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.

[1] https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=530

iii. Unusual applications for DD/TT/PO against cash.

iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.

v. Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid Reporting/Record-keeping Requirements

i. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

ii. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.

iii. An account where there are several cash deposits/withdrawals below a specified threshold level to a avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

i. An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.

ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.

iii. Funds coming from the list of countries/centers which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

i. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.

ii. A customer/company who is reluctant to reveal details about its activities or to provide financialstatements.

iii. A customer who has no record of past or present employment but makes frequent large transactions.

Certain Suspicious Funds Transfer Activities

i. Sending or receiving frequent or large volumes of remittances to/from countries outside India.

ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amountto a different account/center on the same day leaving minimum balance in the account.

iii. Maintaining multiple accounts, transferring money among the accounts and using one account tas a master account for wire/funds transfer.

Certain Bank Employees arousing Suspicion

i. An employee whose lavish lifestyle cannot be supported by his or her salary.

ii. Negligence of employees/wilful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name
- Frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans
- Large deposits immediately followed by wire transfers
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts
- Multiple deposits of money orders, Banker's cheques, drafts of third parties
- Transactions inconsistent with the purpose of the account
- Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities

- A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
- A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
- A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.
- A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
- A customer experiences increased wire activity when previously there has been no regular wireactivity.
- Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- A business customer uses or evidences or sudden increase in wired transfer to send and receivelarge amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.

- Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- Wiring cash or proceeds of a cash deposit to another country without changing the form of thecurrency
- Receiving wire transfers and immediately purchasing monetary instruments prepared forpayment to a third party.
- Periodic wire transfers from a person's account/s to Bank haven countries.
- A customer pays for a large (international or domestic) wire transfers using multiple monetaryinstruments drawn on several financial institutions.
- A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travellers' cheques
- A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when
    - The amount is very large (say over Rs.10 lakhs)
    - The amount is just under a specified threshold (to be decided by the Bank based onlocal regulations, if any)
    - The funds come from a foreign country, or
    - Such transactions occur repeatedly.
- A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)