

JMJ MICROFIN PRIVATE LIMITED
(Formerly Known as Palma Development Finance Private Limited)

KNOW YOUR CUSTOMER (KYC)
AND
ANTI-MONEY LAUNDERING ACTIVITIES POLICY
(“KYC & AML Policy”)

(Revised in the meeting of the Board dated 12/11/2025)

Introduction

As per RBI Know Your Customer (KYC) Direction, 2016 and other applicable RBI norms, all NBFC/ Financial institutions shall have a KYC policy and a policy to prevent money laundering taken up by launderers through transactions with NBFCs/ Financial Institutions.

Money laundering means "any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources". Money laundering is an economic menace which has economic, political and social ramifications and gives opportunities to criminals to expand over countries. India Government has passed Prevention of Money Laundering Act, 2002 and rules to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and to punish those who commit the offence of money laundering.

JMJ MICROFIN PRIVATE LIMITED (Formerly Known as Palma Development Finance Private Limited) has prepared this policy in order to comply with applicable norms and to bring uniformity in collection of documents over branches/ H.O. of the Company.

Scope and application of policy

The policy shall apply to all loans granted by JMJ MICROFIN PRIVATE LIMITED (Formerly Known as Palma Development Finance Private Limited) and instruments issued by the Company for mobilising funds. All branch staff/department heads are expected to comply with the policy. The objectives of the policy are to -

- To lay down explicit criteria for acceptance of customers based on KYC norms issued by RBI.
- 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 prevent criminals from using the Company as an instrument for money laundering activities.
- To ensure early detection of suspicious transactions by establishing appropriate systems for control and detection of activities/customers prohibited under applicable laws/rules/regulations.
- To ensure compliance with applicable laws and regulations relating to KYC and prevention of money laundering.

Definitions

1. **Person:** Person shall have the meaning assigned to it by RBI Act (amended from time to time) 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).
2. **Customer:** means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
3. **Suspicious transaction:** means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

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

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

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

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

6. Prominent public figure (PPF): is a person, such as a politician, celebrity, social media personality, or business leader, who has a certain social position within a certain scope and a significant influence and so is often widely of concern to the public, can benefit enormously from society, and is closely related to public interests in society.

7. Aadhaar number: Aadhaar/ Aadhaar number means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

8. Money laundering: means any process or activity connected with proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property.

9. Proceeds of crime: means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property;

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

10. Valid Customer Proof (VCP): Valid customer proof means documents which are legally valid and/or legally enforceable in India and has not expired during the period of submission and which are collected by the Company for following purpose-

- To identify the customer as a citizen holding proof of his/her nationality
- To track the location based on address mentioned
- To avoid misuse of identity
- To record other basic details like age, father name, etc.

11. Certified copy of VCP/Temporary VCP: means the copy of ID proof/KYC documents self-attested by customer in presence of branch staff and verified by Branch staff after comparing with Original and which bears the seal/remarks "Verified" along with sign of the verifying official.

12. **Principal Officer:** Principal officer means an officer appointed under Prevention of Money Laundering Act and/or under RBI norms for the purpose of reporting suspicious transactions or implementing the KYC & AML policy. In the event that an employee violated Company's rules on measures to prevent money laundering and terrorist financing without legitimate reason, the Principal Officer may give him/her a warning or take other appropriate action in accordance with the nature of the offence.

KYC & AML Standards

JMJ MICROFIN PRIVATE LIMITED (Formerly Known as Palma Development Finance Private Limited) KYC & AML Standards would include the following elements-

1. Customer acceptance
2. Customer identification
3. Risk management
4. Monitoring of transactions & ongoing due diligence.
5. AML initiatives

1.Customer Acceptance policy:

a. Account opening and identification

The Company shall ensure that -

- i.No account is opened in anonymous or fictitious/benami name.
- ii.Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the FIs in categorizing the customers into low, medium and high-risk ones.
- iii.Unique Customer ID shall be allotted to a customer and no need of separate KYC for customers already existing with KYC compliant account.
- iv.Documents and other information to be collected from different categories of customers depending on perceived risk and the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time.
- v. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking.
- vi. The Company has suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.
- vii. Customer ID will not be opened or Transactions are not conducted with customers who fail to co-operate with Customer Due diligence process and documentation processes. The bank/FI may also consider closing an existing account under similar circumstances.

b. Restrictions/Prohibition on lending to certain categories of customers/sectors

- i. Loan to staff members: Loans to staff members shall have same terms and conditions applicable to common public. Any deviation in terms shall require prior approval of Managing Director/Wholetime Director Board of Directors. Unpaid amount of interest or principle or both shall be recovered from the salary account of the employee/staff as may be agreed between the staff, HR Department and the Company.
- ii. Loans to borrowers in "black list" or having history of pledging spurious/stolen gold ornaments or has a background of financial frauds or who has deliberately tried to cheat the Company and created any loss to the Company, shall not be sanctioned. The Company shall electronically and/or physically maintain an updated list of customers identified by the Company as "persistent

defaulter” or “blacklisted”/ “Caution” customers. The Company may also check whether the customer is blacklisted or identified as caution customer by RBI/any credit agencies/ government/competent authorities. Where the Company officials fails to identify at the first instance, but realises that the customer is a person with such a background, then procedures for freezing or blocking of customer ID of that person shall be initiated by the concerned officer. Relevant clauses of auction policy, fair practice code and NPA Policy shall be referred for more clarity.

- iii. Loans to persons/customers having higher than normal risk shall be avoided/ reduced. Eg. Loans to goldsmiths, Jewellery owner etc or any other persons.

In case of existing business relationships, if the Customers are not KYC compliant, the Company will take necessary measures to carry out necessary actions to comply with the requirements and where the Company fails to do so, it will take necessary measures to either terminate the existing relationship or carry out necessary actions to partially freeze the business relationship in accordance with the provisions of the RBI's Guidelines on “Know Your Customer” and Anti-Money Laundering Measures, as amended from time to time, have been complied with.

If an existing KYC compliant Customer desires to open another account, there would be no need for submission of fresh proof of identity and/or proof of address for the purpose.

2.Customer Identification Procedure

The Company shall ensure adherence of Customer Identification Procedure as prescribed by the Reserve Bank of India from time to time. The Company would obtain the KYC documents for second time whenever there is doubt about the authenticity/veracity or the adequacy of the previously obtained Customer identification data. If Aadhaar card is taken as KYC, the Company would satisfy itself about current address by obtaining required proof. The Company also have the process of allotting Unique number for easy identification of all the relationships of any Customer with the Company. Information collected for the purpose of opening of account would be kept as confidential and would not be divulged to outsiders for cross selling or any other purpose other than for the statutory requirement of sharing the Customer account details with credit information agency or any other requirements under RBI norms. Information sought from the Customer would be relevant to the perceived risk and would not be intrusive.

Third party products/services

The Company may deal with third party products or services which is in accordance with applicable RBI norms. The third-party service providers shall be NBFCs, Scheduled Commercial Banks, Regional Rural Banks, All India financial institutions, RNBC, MNBC, PPI issuers, payment system providers, MTSS providers or authorised persons registered with RBI or registered under Banking Regulation Act, allowed to perform business activities with the Company as per applicable RBI norms/laws. The Company may rely on the due diligence exercise conducted by third party on purchase/availing of product or service of Third-Party service providers and shall cause to collect all due diligence reports/records within 3 days of establishing customer relationships. In order to ensure the intention of this policy, the Company shall follow-up with third party to ensure all records are in proper order and as per requirements of this policy/ RBI norms. Identity of customers conducting transaction of amount of Rs.50,000/- and above shall verified using PAN and transactions shall be undertaken through proper banking channels.

3.Risk Management

- The branch manager/Asst manager/officer shall ensure that each loan is given a risk grade based on the background and credit worthiness of the customer. The branch shall ensure that gradation is done as normal risk, high risk and low risk on the application form itself based on the information collected from the customer.

- List of individuals engaged in financial frauds shall be circulated to branches/staffs to reduce chances of risk via frauds.
- Proper verification of originals with copy of KYC documents and test checking the telephone numbers provided by customers is strongly suggested.
- Credit score analysis is strongly suggested in cases of high value loans and loans to individuals with high-risk background.
- Strict adherence to KYC norms shall be ensured by the Company/Branches
- The interest rates should be subject to change based on perceived risk and/or as the situation warrants and are subject to management decision based on the merit of individual cases. More the loan amount, more the risk involved. Where the loan amount is high, more care shall be exercised.
- Purity of gold shall be analysed using appropriate machines/systems and shall be subject to audit by internal audit team or special audit team. It is advised to ensure purity of gold by two officers in the branch, where the loan amount is high. It is important to note that gold loans are given against security of gold ornaments and lack of purity will affect the Company adversely.
- Existing debts of the borrowers should be analysed before sanctioning of the loan.
- The internal audit team shall verify the risk aspects of a loan/customer along with routine matters and give their suggestions to management.
- Loan policy, NPA policy, interest rate policy, Fair practice code, KYC policy of the Company shall be read and understood by employees. The branches/staff members may give suggestions to the management regarding risk management based on their own experience/qualification.
- Suspicious transactions shall be reported to the concerned authorities without delay.

4. Monitoring of Transactions & Due diligence

All transactions above Rs.50,000/- shall be subject to monitoring and due diligence at initial stage and ongoing due diligence shall be exercised mandatorily in case of loans exceeding Rs.100,000/-. The Company would strive to have an understanding of the normal and reasonable activity of the Customer through personal visits and by observing the transactions and conduct of the account in order to identify transactions that fall outside the regular pattern of activity – unusual transactions.

The Company shall collect the following from an individual before opening of account/initiating transaction –

- a. Valid Customer proof (VCP) as specified in Annexure I.
- b. Recent photograph
- c. Contact numbers (Mobile and land phone).
- d. Email Id.
- e. Any other documents depending upon the scheme.

The Company shall make use of online Aadhaar verification (e-kyc of UIDAI) and offline verification to ensure compliance with this policy. The Company may outsource verification to a third party provided such outsourcing is as per RBI norms and applicable laws. However, the branch staff and Company shall be the ultimate persons to ensure compliance with applicable KYC norms.

The following incidents of counterfeit currency at the cash counters shall be recorded and repeated occurrence shall be reported.

- Bulk counterfeit currency of more than 10 pieces at a time;
- Repeated event within a week from a collection executive or Customer;

All such transactions would be reported to and reviewed by Principal Officer – PMLA who would enquire into the matter and decide whether the transaction would qualify to be termed as a suspicious transaction. The Principal Officer - PMLA shall file the Suspicious Transaction Report (STR) with the Director, Financial Intelligence Unit-India (FIU-IND) within 7 days of identifying them. After filing STR, transactions would be allowed to be continued in the account unhindered and the Customer would not be tipped in any manner. All CTR/STR would be filed electronically or as per the norms stipulated

by FIU-IND from time to time. Financial Action Task Force (FATF) statements regarding countries with deficient AML/CFT would be verified and caution would be exercised with Customers who conduct business activities in these countries.

Annexure II to this policy contains suggestive list of transactions which could be considered as “Suspicious transaction”. The principal officer shall exercise reasonable diligence while qualifying a transaction as “suspicious transaction” as the aforesaid list is suggestive in nature. The decision shall be based on facts, figures of the transaction and also behaviour of person(s) under suspicion.

All the units reporting the unusual transactions to Principal Officer – PMLA would be subjected to audit by Internal Audit Department.

The Company shall collect PAN for all loan customers transacting at Rs.5 lakhs and above. Any cases, where PAN is not available with Company, the customer shall be monitored closely.

The Company shall undertake ongoing due diligence of customers to check whether their financial status and sources of funds are consistent the records of the customers. The Company shall have adequate systems to monitor any extraordinary change in frequency of transactions or suspicious transactions in the account. The risk monitoring systems shall be based on level of risk. High risk accounts shall be closely monitored when compared to low-risk accounts. The branch staff shall note that the limit of Rs.100,000/- is mandatory and it is strongly advised to take up ongoing due diligence even in case of difference of up to Rs.50/- less from the limit. (ie.Rs.99,950/-).

5.AML Initiatives

As aforesaid procedures take both human intelligence and technical support to spot the warning signs, employee training programmes, internal communications and monitoring systems should all be up to date on the latest risks. The concerned departments and Officers shall investigate any suspicious activity and keep thorough records of decision on whether to freeze funds and file a report with the relevant authorities. If no report is filed, it is essential that the reasons for this are fully documented. Internal audit and external audit shall also be fully effective to boost the AML initiatives of the Company. Internal control structure is critical to the safe and sound functioning of the banking organization and its risk management system. AML initiatives of the Company shall be cost effective. Therefore, establishing and maintaining an effective system of controls, including the monitoring of official lines of authority and ensuring the appropriate separation of duties, need to be one of management’s priority while doing business. Reporting relating to money laundering/suspicious activities should be reported to Board in order to bring in improvements in policies.

AML initiatives of management could be brought under following points-

1. Best Governance practices
2. Risk identification, assessment, and mitigation
3. Policies and procedures
4. Customer identification and due diligence
5. Transaction monitoring
6. Reporting
7. Communication and training
8. Continuous improvement and testing
9. Effective Internal and external audit

For aforesaid purposes the senior and middle level managers /Department heads shall

- i. Communicate and reinforce the AML/KYC compliance culture established by the board, and implement and enforce the board-approved AML/KYC compliance program requirements to ensure compliance with applicable RBI norms and other policy requirements
- ii. Monitor the AML/KYC risk assessment
- iii. Circulate all AML/KYC-related policies and instructions
- iv. Implement Board approved action plans
- v. Ensure staff accountability for their operations and inculcating compliance culture in employees/staff

For JMJ Microfin Private Limited

Sd/-

Director

Annexure I

Valid Customer Proof

A. Group/ Personal/ Term Loan - Individuals

Certified copy of all the following documents shall be the VCP to be collected and verified with original-

- i. PAN (Mandatory if the loan amount is Rs. 50,000/- or more)
- ii. ID proofs of Applicant and Guarantor (if any) (containing address).
- iii. Bank statement for at least 6 months.
- iv. Any other document as may be required as per the scheme requirements.

Where due to some reasons, the VCP submitted does not contain present/permanent address of the customer, then any one of the following “proof of address” shall be collected and verified (in the manner mentioned in the policy) in addition to the above-

- a. Utility bill (electricity bill, mobile bill, telephone bill etc) not older than two months, which contains present/ permanent address;
- b. Letters/certificates/statements issued by State Government/Central Government/Statutory or regulatory bodies/PSU/Scheduled commercial banks containing present/updated address of the customer;
- c. Any other VCP containing present/ permanent address;

All documentation shall also be subject to Loan policy, Fair Practice Code, Interest rate policy etc.

B. Non-Individuals

KYC norms shall be followed in case of non-individuals. The following shall be complied with depending upon the constitution of the applicant/customer-

	Type of Non-individual	Documents
1.	Companies	<p>Certified True Copy* of all of the following documents-</p> <ol style="list-style-type: none">a. Certificate of incorporation (as on date) issued by Registrar of Companies (MCA) and Certificate of registration (as on date) under any other regulator, if applicable.b. Latest Memorandum and Articles of Association of the Company.c. Resolution (on letterhead) passed by the Board of Directors for opening of account/initiating transaction with Company and authorizing one or more person to operate the account/perform transactions on its behalf;d. PAN of the Company.e. List of Directors as on date. <p>*Certified True Copy here shall mean copy of document certified as true by at least two Directors of the company.</p>

		<p>*In case of companies having 3 Directors and authorising more than 1 persons as authorised signatory, it is strongly advised to ensure that at least one Director certifying the resolution is a different person.</p>
2	Partnership Firm	<p>The following documents shall be collected-</p> <p>1.Certified True Copy* of all of the following documents-</p> <ol style="list-style-type: none"> a. Registration certificate issued by Registrar of firms and Certificate of registration (as on date) under any other regulator, if applicable. b. Resolution (on letterhead) authorising one or more person to operate the account/perform transactions on its behalf c. Partnership Deed d. PAN. <p>and</p> <p>2. Valid Customer Proof (VCP) (as discussed in Para A for individuals) of authorised signatory.</p> <p>*Certified True Copy here shall mean copy of document certified as true by at least two partners of the firm.</p> <p>*In case of firm having 3 partners and authorising more than 1 person as authorised signatory, it is strongly advised to ensure that at least one Partner certifying the resolution is a different person.</p>
3.	Trusts	<p>The following documents shall be collected-</p> <p>1.Certified True Copy* of all of the following documents-</p> <ol style="list-style-type: none"> a. Registration certificate b. Resolution (on letterhead) authorising one or more person to operate the account/perform transactions on its behalf. c. Trust Deed d. PAN or Form 60 e. Power of attorney authorising the person(s) to carry out transactions for and on behalf of the trust. <p>and</p> <p>2. Valid Customer Proof (VCP) (as discussed in Para A for individuals) of authorised signatory.</p> <p>*Certified True Copy here shall mean copy of document certified as true by at least two trustees.</p> <p>*In case of trust having 3 trustees and authorising more than 1 persons as authorised signatory, it is strongly advised to ensure that at least one trustee certifying the resolution is a different person.</p>
4.	Any other body of individuals or juridical	<p>The following documents shall be collected-</p>

<p>persons or unincorporated association not covered in above classification.</p>	<ul style="list-style-type: none"> a. Signed Request letter of Head of the association/BoI. b. Valid proof showing the person signing the letter is the head of association/BOI. c. Certified true copy of Resolution certified as true and forming part of the minutes of the meeting of the managing body. d. PAN, (in case no PAN applicable, then any other valid proof indicating identity of the association/BoI in records of regulatory authority). e. Power of attorney/Authorisation letter authorising the person(s) to carry out transactions for and on behalf of the trust. f. Any other document as may be required to prove the existence of such association/BoI.
---	--

Annexure II

Reasons for Suspicion

1. Persistent effort to avoid submission of required documents and information within set time limits.
2. Unexpected flow of income from sources not reported and known to have existed as per records submitted with Company.
3. Close relatives or friends of known criminals.
4. Providing fake documents for opening of account/transactions.
5. Activity inconsistent with what could be expected from declared financial background/status/business. Aggregate Value of transactions or frequency of transaction inconsistent with financial position of the customer.
6. No bonafide purpose for transaction.
7. Unwillingness to meet in person, when called for information or payment of interest/principal.
8. Continuous absence from residence address submitted with Company during period of repayment without any reason.
9. Unusual or unjustified complexity.
10. Hesitation to provide bank details and high frequency of cash transactions.
11. Failure to attend calls on a continuous basis.
12. Hesitation to sign documents or declarations relating to loan documents.
13. Continuously pledging gold ornaments of low purity/fake gold which will be revealed only on a later stage, on advanced testing.
14. Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnishes a plausible reason for immediate withdrawal.
15. Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.
16. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
17. A customer who has no record of past or present employment but makes frequent large transactions.
18. Sudden surge in activity level.
19. Same funds being moved repeatedly among several accounts.
20. Approaching a branch far away from residence of the customer.
21. Giving request for payment to third party without any reason.
22. Usage of loan amount for purposes other than those intimated to the Company.
23. Request for change of address frequently without any justifiable reason.
24. Requesting for loans of huge amount split into small amounts to avoid reporting under applicable laws.
25. Where the person is a politically exposed person without a source of income that justifies the amount transacted over the accounts.
26. Persuading the staff to excuse him/her from major documentation and due diligence.
27. Offering bribe/money or agreeing to pay money or provide benefits to employee or trying to make friends/personal relationships with employees of the Company outside the premises/inside the office premises or compelling for acting leniently.
28. Customers coming from places/organisations known for money laundering or having track record in criminal activities and acts in a manner that creates reasonable suspicion in the mind of an employee of normal prudence.
29. Customers bringing counterfeit currency exceeding 10 pieces at a time or trying to pay bulk counterfeit currency in multiple accounts at same time.
30. Customers who fail to appear in the branch or before collection agent after loan sanction and always tries to make transactions through his agent/attorney without a bonafide reason.
31. Customers who do not have good credit history owing to failure in repayment of loans in financial institutions/banks.
32. Encashment of loan through fictitious bank account.

33. Any other case where the customer acts in way to hide required information, his identity, actual purpose of funds, source of funds, background etc or engages in activities different from a normal customer.

-----End of Document-----