Leveraging Digital India to Help Micro Enterprises Grow

Vreedhi Financial Services Private Limited

KNOW YOUR CUSTOMER (KYC)

Leveraging Digital India to Help Micro Enterprises Grow

Prepared By	Designation	Signature
Dipesh Arya	Head – Finance & Accounts	

Reviewed By	Designation	Signature
P.N. Srinivasa Rao	COO	

Adopted by Board	
Director (On behalf of the Board of Directors)	Shamik Trehan, Chairman

PREAMBLE:

Policy has been formulated in line with the Know Your Customer (KYC) Directions, 2016, Anti-Money laundering (AML) Standards and Combating the Financing of Terrorism (CFT)/ Obligation of NBFCs under Prevention of Money Laundering Act (PMLA), 2002 and Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and such other rules framed thereunder (including any statutory modification(s) or re-enactment(s) thereof for the time being in force). It imposes obligations on banking companies, financial institutions and intermediaries to verify identity of clients, maintain records and furnish such information in prescribed form to Financial Intelligence Unit - India (FIU-IND).

The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards to protect the financial system against the threat of money laundering/terror financing and frauds and has advised all the Regulated Entities to put in place a Board Approved KYC Policy and also to ease the burden on the prospective customers in complying with the KYC requirements

The sole objective of the apex Bank, RBI is to prevent Regulated Entities being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines equally mandates 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 the Company to manage its risks prudently. Accordingly, it aims to enable the entities to follow Customer Identification Procedure (CIP) in true spirit while undertaking transactions either by establishing an account-based relationship or otherwise and timely monitor their transactions.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company has been approved by the Board of Directors.

This policy is applicable to all categories of products and services offered by the Company. Company shall ensure at all times that decision-making functions of determining compliance with KYC norms are not outsourced.

This policy shall be in force from immediate effect.

OBJECTIVES, SCOPE AND APPLICATION OF THE POLICY

The Policy aims to fulfill following objectives:

1. To prevent criminal elements from using Company for money laundering activities
2. To enable Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risks prudently
3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures
4. To comply with applicable laws and regulatory guidelines
5. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures. This KYC Policy is applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time.
6. The senior management for the purpose of KYC Compliance shall mean the executive directors including MD or WTD and Designated Director, Nodal Officer (NO), Grievance Redressal Officer (GRO), Principal Officer (PO), Compliance Officer (CO) and such other head/chief of all departments, including functions like Business, Operations, Credit, Collections etc.
7. The Board of Directors through Designated Director, shall ensure an effective implementation of policies and procedures and shall review such policies, control, effectiveness, training, legal and regulatory requirements, etc. through Internal Auditor in the company
8. The Principal and/or Compliance Officer alongwith Company Secretary shall ensure to put up such audit notes and its compliances on quarterly basis, in the Board or Audit Committee.
9. **Elements:**
    a. Customer Acceptance Policy (CAP)
    b. Risk Management
    c. Customer Identification Procedures (CIP)
    d. Other Provisions

KEY ELEMENTS:

I. CUSTOMER ACCEPTANCE POLICY ('CAP"):

Below mentioned norms and procedures will be followed by the Company in relation to its customers who approach for availing the financial facilities. While taking decision to grant any one or more facilities to customers as well as during the continuation of any loan account of the customer, the following norms shall be adhered by the Company at all times. However, the Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

1. The Company's CAP lays down the criteria for acceptance of Customers:

i. No loan shall be disbursed to anonymous or fictitious/benami name.

ii. No loan shall be disbursed where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

iii. No loan is disbursed where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

iv. The mandatory information to be sought for KYC purpose while disbursing the loan and during the periodic updation, is specified.

v. Optional/Additional Information, is obtained with the explicit consent of the customer after the loan is disbursed.

vi. Company shall apply CDD while disbursing the loan for first time. If KYC compliant customer desires to avail another loan, there shall be no need for fresh CDD. Such CDD shall be done at UCIC level (Unique Customer Identification Code) Such exercise shall be needed for all the joint customers , while disbursing the loans.

vii. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

viii. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

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

x. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature.

- 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

II. RISK MANAGEMENT

i) The levels of Risk Categorization would be Low, Medium and High Risk. It shall be based on customer's identity, social/financial status, nature of business activity, information about the business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities will also be factored in.

Category A: High Risk Customers includes:

a) Non-Resident Customers;
b) High net worth individuals without an occupation track record of more than 3 years;
c) Companies having close family shareholding or beneficial ownership;
d) Firms with sleeping partners;
e) Politically exposed persons (PEPs) of Indian/ foreign origin;
f) Person/Entity whose name appears in the sanction lists circulated by RBI
g) Person with dubious reputation as per public information available;
h) Trusts (except trusts appropriately set up under a specific regulation);
i) Societies;
j) Charitable Institutions;
k) NGOs and other organizations receiving donations from within or outside the country

Intensive due diligence will be taken and exercised in respect of those customers who happen to be high risk profile. Such cases will include those where the sources of funds to be used for business operations or sources to repay the loan to the Company are not clearly disclosed or cannot be ascertained from the financial statements submitted by the customer to the Company.

Category B: Medium Risk Customers includes:

a) Self- employed professionals other than High Net worth individuals.

b) Self-employed customers with sound business and profitable track record for a reasonable period;
c) High Net worth individuals with occupation track record of more than 3 years

Category C: Low Risk Customers includes:

a) Persons having own accommodation as residential address for over 5 years;
b) People belonging to lower economic strata of the society whose accounts show small balances and low turnover

III. Customer Identification Procedures ("CIP"):

Customer Identification means undertaking CDD measures including identifying and verifying the customer on the basis of one of the *Officially Valid Documents (OVD) in the following cases:

(a) Application for loan by the customer
(b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained
(c) When the company has reason to believe that a customer is intentionally structuring a transaction into a series of transactions

For undertaking CDD, the company shall obtain the following from an individual or an individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number or
(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address;
Where the company shall ensure to redact or blackout the Aadhaar number
and
(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the company

The company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required

"***Officially Valid Document***" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

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

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

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

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

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

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

Video based Customer Identification Process (V-CIP)

VFS does not intend to carry on V-CIP at present, annexure for the same shall be added to the policy at a suitable time.

KYC verification done by one branch/office of the company shall be valid for transfer of the account to any other branch/office of the same company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

The CDD measures for Sole Proprietary Firms, Legal Entities and Identification of Beneficial Owner are given under Annex – 1 of this policy.

Since the company is not a deposit taking NBFC, Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs) is not applicable to VFS.

On-going Due Diligence

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 the source of funds.

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

(a) REs shall carry out

i. CDD, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

ii. In case of Legal entities, the company shall review the documents sought at the time of opening of account and obtain fresh certified copies.

Provided, REs shall ensure that KYC documents, as per extant requirements of the Master Direction, are available with them.

(b) The company may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the customer is required to establish their bona-fide. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

(c) The company shall ensure to provide acknowledgment with date of having performed KYC updation.

(d) The time limits prescribed above would apply from the date of disbursement/ last verification of KYC.

Since the company would not disburse the loans to non-face-to-face customers or by application made through professional intermediaries, the regulations for the same will not be applicable to the company.

The disbursement of loan to Politically Exposed Persons (PEPs) may be done as below,

(a) sufficient information including information about the sources of funds, details of accounts of family members and close relatives is gathered on the PEP;

(b) the identity of the person shall have been verified before accepting the PEP as a customer;

(c) the decision to disburse a loan to a PEP is taken at a senior level

(d) all such customers are subjected to enhanced monitoring on an on-going basis;

(e) in the event of an existing customer or the beneficial owner of an existing customer subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

(f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner

IV. Other Provisions

Record Management

Customer Account Information shall be maintained, preserved and reported strictly in accordance with the applicable provisions of PML Act, rules made thereunder and any clauses/provisions contained in KYC Master Directions to that effect.

Reporting Requirements to Financial Intelligence Unit – India (FIU-IND)

The company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

The reporting of CTR and STR shall be done in accordance with the rules framed thereunder. The company shall not put any restriction on operations in the loan accounts where an STR has been filed. The company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

Necessary and required robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers, shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Requirements/obligations under International Agreements

Company shall not have any account in the name of individuals/entities appearing in the lists suspected of having terrorist links, approved by and periodically circulated by the United Nations Security Council (UNSC).

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated March 14, 2019 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

Clause related to consideration, recommendations etc. required as per FATF shall be adhered to as per the KYC Master Directions or any other directions issued by RBI.

Secrecy Obligations and Sharing of Information

The company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

Sharing KYC information with Central KYC Records Registry (CKYCR)

Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Act, as required by the revised **KYC Templates** prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised CERSAI to act as, and to perform the functions of the CKYCR. Company shall upload the KYC data pertaining to all the individual accounts with CERSAI.

Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, the company shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F

UCIC

Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by NBFCs.

Introduction of New Technologies

Adequate attention shall be paid by the company to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

Selling Third Party Products

VFS does not intend to carry on any such activities. However, the company shall ensure compliance to all clauses of KYC Master Direction or such other directions, in case the company intend to carry on such activities. Necessary amendment shall be made to the policy, if required, at an appropriate time.

Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front line staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the company, regulation and related issues shall be ensured.

Money Laundering and Terrorist Financing Risk Assessment by the Company:

(a) The Company shall carry out Risk Assessment to identify and assess the risk and accordingly take effective measures to mitigate.

The assessment process should consider all the relevant risk factors. While preparing the internal risk assessment, Company shall take cognizance of the overall sector-specific vulnerabilities, if any.

(b) The risk assessment shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. Further, the periodicity of risk assessment shall be determined by the Board in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board and should be available to competent authorities and self-regulating bodies.

Company shall also apply a Risk Based Approach (RBA) for mitigation and management of the identified risk. Further, Board shall timely monitor the implementation of the controls and enhance them if necessary.

Annex – 1 CDD measures

Proprietorship Concerns	Apart from Customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice • Registration certificate • Certificate/license issued by the Municipal authorities under Shop & Establishment Act, • Sales and income tax returns • CST/VAT/GST certificate (provisional/final) • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. • IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. • Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities • Utility bills such as electricity, water, landline telephone bills etc. (in business name) The company if satisfied that it is not possible to furnish two such documents and at its own discretion, accept only one of these documents as proof of business/activity provided the company undertakes contact

	point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
Partnership firms/Trust	• Registration certificate • Permanent Account Number of the partnership firm/Trust • Partnership deed/Trust Deed; • Documents relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Companies	• Certificate of Incorporation • Memorandum & Articles of Association; • Permanent Account Number of the company • A resolution from the Board of Directors and power of attorney granted to its managers, officers, employees to transact on its behalf.
Unincorporated Association or Body of Individuals	• Resolution from the Managing Body of such association or body of individuals • Permanent Account Number • power of attorney granted to transact on its behalf • Documents relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
societies, universities and local bodies like village panchayats	• Document showing name of the person authorised to act on behalf of the entity; • Documents of the person holding an attorney to transact on its behalf and • Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken keeping in view the following:

(a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Annex-2 Digital KYC

Process for capturing live photo

(i) The company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Company.

(ii) The access of the Application shall be controlled by the Company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

(iii) The Customer, for the purpose of KYC, may visit the location of the authorized official of the Company or vice-versa. The original OVD shall be in possession of the customer.

(iv) The Company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

(v) The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

(vi) Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt

in the mobile device shall be there while capturing the live photograph of the original documents.

(vii) The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

(viii) Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

(ix) Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

(x) The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

(xi) Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the transaction-id/reference-id number of the process. The authorized officer

shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

(xii) The authorized officer of the company shall check and verify that: (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

(xiii) On Successful verification, the CAF shall be digitally signed by authorized officer of the company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.