

KHUSHBU AUTO FINANCE LIMITED

**KNOW YOUR CUSTOMER GUIDELINES ("KYC")
AND
ANTI-MONEY LAUNDERING STANDARDS ("AML")
UNDER PREVENTION OF MONEY LAUNDERING ACT ("PMLA") 2002**



1. GLOSSARY

AML	Anti-Money Laundering
CAP	Customer Acceptance Policy
CBIC	Central Board of Indirect Taxes and Customs
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest
CIBIL	Credit Information Bureau (India) Limited
CIP	Customer Identification Procedures
CTF	Counter-Terrorism Financing
CTR	Cash Transaction Report
FIU-IND	Financial Intelligence Unit-India
KYC	Know Your Customer
NBFC	Non-Banking Financial Companies
NPO	Non-Profit Organization
NRI	Non-Resident Indian
OVD	Officially Valid Document
PEP	Politically Exposed Person
PIO	Person of Indian Origin
PMLA	Prevention of Money-Laundering Act
RBI	Reserve Bank of India
STR	Suspicious Transaction Report
UCIC	Unique Customer Identification Code
UIDAI	Unique Identification Authority of India
WMD	Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act

2. INTRODUCTION

The Central Government of India, vide its notification no GSR 436 (E) dated July 1, 2005, had enacted Prevention of Money Laundering Act, 2002 (PMLA) to prevent conversion of illegal money to legal money, directly or indirectly and to curb threat to bank and financial institutions and to formulate the legal framework on Anti-Money Laundering and Countering Financing of Terrorism.

Reserve Bank of India has further issued Master Direction- Know Your Customer (KYC) Direction, 2016 including 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.

The Know Your Customer, Anti-Money Laundering and Counter-Terrorism Financing Policy (the "Policy") applies to the Company, its Subsidiary, branches, if any and its Group. This Policy is consistent with and effectively implements the Reserve Bank of India's various guidelines and enactments including Master Directions - Know Your Customer (KYC) Direction, 2016 (As amended from time to time). The Policy seeks to establish the procedures that Khushbu Auto Finance Limited (hereinafter referred to as 'KAFL' or 'Company') shall be following while undertaking any transaction, either through account-based relationships or otherwise, and while monitoring such transactions. The content of the policy shall always be read in tandem/auto-corrected with the changes/modifications which shall be advised by RBI from time to time.



KAFL shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications, if any necessary, to this Policy to conform to the standards so prescribed.

Objective of this Policy:

- Protect the Company from being used for money laundering or funding terrorist activities;
- Comply with the letter and the spirit of applicable RBI Master Direction on Know Your Customer (KYC) including comprehensive guidelines on Know Your Customer (KYC) norms and Anti-money Laundering (AML) Laws as applicable to the Company;
- Be alert to and escalate suspicious activity;
- Cooperate with AML-related law enforcement and regulatory agencies to the extent permitted under applicable laws;

The company shall specify as to who constitute 'Senior Management' and allocate responsibilities for implementing the Policy; and the Company shall also undertake independent evaluation of the compliance functions of the Policies and have in place concurrent/internal audit system to verify adherence to the same, and shall submit quarterly audit notes to the Audit Committee.

3. POLICY REVIEW AND APPROVAL

The Policy shall be reviewed/ approved time to time as and when required by the Board of Directors of the Company, and, more frequently, if changes are required as per amendments in the applicable rules, regulations.

4. DEFINITIONS

A. Customer:

Customer shall mean and include all the person(s) who are engaged in any financial transaction or activity with KAFL and shall include the person on whose behalf the person who is engaged in the transaction or activity, is acting. For clarification, "Customer" shall include all parties to the transaction, i.e. co-borrowers, guarantors, persons/entities executing the security documents etc.;

B. Non-face to face customers:

Those Customers who open accounts or engages in any transaction or activity without visiting the branch/offices of the KAFL or meeting the officials of KAFL;

C. Transaction:

Transaction shall mean a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- Opening of an account;
- 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;
- Entering into any fiduciary relationship;
- Any payment made or received, in whole or in part, for any contractual or other legal obligation or
- Establishing or creating a legal person or legal arrangement

D. Customer Due Diligence (CDD):

CDD means the procedure for identifying and verifying the customer and the beneficial owner.

E. Customer identification:

Customer Identification means undertaking the process of CDD.



F. On-going Due Diligence

On-going Due Diligence means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

G. Beneficial Owner:

- i. where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation.—For the purpose of this sub-clause—

"Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;

"Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

- ii. where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than ten per cent of capital or profits of the partnership or who exercises control through other means;

Explanation.—For the purpose of this clause,

"Control" shall include the right to control the management or policy decision;

- iii. where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent of the property or capital or profits of such association or body of individuals;

- iv. where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

- v. where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

- vi. where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

H. KYC Identifier:

KYC Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry

I. Suspicious transaction:

Transaction 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 PML Act, 2002 or specified in WMD Act, 2005, 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.



J. Officially Valid Document ("OVD"):

OVD shall include the passport, the driving license, 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, letter issued by the National Population Register containing details of name and address. Provided that,

- i. 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.
- ii. 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: -
 - a. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - b. property or Municipal tax receipt;
 - c. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - d. 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 license agreements with such employers allotting official accommodation.
- iii. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'ii' above
- iv. 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 1 - 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.

K. Certified Copy:

Certified copy shall mean a copy obtained by the Company by comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document (as defined in the RBI Master Direction) so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company.

L. Digital KYC:

Digital KYC shall mean capturing the live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company.

M. Equivalent e-document:

It means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

N. Video based Customer Identification Process (V-CIP):

V-CIP Process shall mean an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and

maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face Customer Identification Process.

O. Politically Exposed Persons (PEPs):

PEPs mean Individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials, etc.

P. FATCA

It means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S Tax payers or foreign entities in which U.S Tax payers hold a substantial ownership interest.

Q. Group

The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).

R. Payable-through accounts

The term payable-through accounts refer to correspondent accounts that are used directly by third parties to transact business on their own behalf.

S. Non-profit organisations (NPO)

NPO means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013)

All other expressions, unless defined herein, shall have the same meaning as have been assigned to them in the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the PML Act, 2002, the PML (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Reserve Bank of India - Master Direction - Know Your Customer (KYC) Direction, 2016, and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

5. COMPLIANCE OF KYC POLICY

For the purpose of Compliance of KYC Policy, Risk Management Committee is made responsible. Risk Management Committee will be authorized to make decisions in this regard. It is to be ensured that decision-making function of determining compliance with KYC norms will not be outsourced.

Independent evaluation of Compliance of policies, procedures with legal and regulatory requirement will happen. Auditors to verify the compliance to AML and KYC policies & submit quarterly reports with action taken to Audit Committee.

6. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise annually. The Company will take cognizance of the overall sector-specific vulnerabilities shared by the regulator/supervisor. Company shall identify, assess and take measures to mitigate its money laundering and terrorist financing risk for customers, countries or geographic areas, products, services, transactions or delivery channels, etc.



The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and will make Board approved policies, controls and procedures in this regard. Monitoring of the implementation of the controls will be ensured and same will be enhanced where necessary.

7. KEY ELEMENTS OF POLICY

The Company is hereunder framing its KYC Policy incorporating the following four key elements:

- A. Customer Acceptance Policy (CAP)
- B. Risk management
- C. Customer Identification Procedures (CIP)
- D. Monitoring of Transactions

A. Customer Acceptance Policy (CAP)

The guidelines for Customer Acceptance Policy (CAP) followed by KAFL are given below:

- i. No account or transaction shall be opened/entered into in anonymous or fictitious/ benami name(s);
- ii. No account to be opened where the Company is unable to apply appropriate CDD measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company;
- iii. No transaction or account-based relationship shall be undertaken without following CDD procedures;
- iv. All mandatory information sought for KYC compliance shall be specified while opening an account and during the periodic updation. Any additional information, the requirement of which is not specified in this policy or RBI Master Directions, shall be obtained with the explicit consent of the Customer;
- v. The Company shall ensure that Customers are allotted a UCIC, to unify all the account of Customers. If an existing KYC compliant Customer wishes to open another account, there shall be no requirement for a fresh CDD procedure, without prejudice to such periodic updation as provided in the Policy;
- vi. CDD Procedure shall be followed for all the parties of the transaction, including borrower, co-borrowers, guarantors, persons/entities executing the security documents, etc.;
- vii. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority;
- viii. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000);
- ix. The Company shall ensure that the identity of any Customer does not match with any person whose name appears in the sanctions lists as circulated by Reserve Bank of India from time to time;
- x. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority i.e. CBIC;
- xi. The Company shall ensure that the CAP does not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged;
- xii. No account shall be opened and/or held on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the Company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or



- understand true nature and purpose of transaction(s), should not be allowed to open an account on behalf of a client
- xiii. Upon apprehension or suspicion of money laundering or terrorist financing, and upon reasonable belief that performing the CDD process will tip-off such a Customer, the Company shall not pursue the CDD process, and instead file an STR with FIU-IND;

B. Risk Management

The Company evaluates its Customers through a risk-based approach, categorizing the Customers as Low risk, Medium risk and High risk, using the following parameters:

- i. Customer's identity
- ii. Nature of business of the Customer
- iii. Information about the customer's business and their location
- iv. Geographical risk covering customers as well as transactions
- v. Delivery channel used for delivery of products/services
- vi. Social and financial status
- vii. Quantum & tenure of Loan facility applied for and proposed schedule for repayment of Loan
- viii. Customer Type (Partnership, Pvt. Ltd. Public Ltd., Trust, NGOs etc.)
- ix. Transparency in ownership & control structure
- x. Type of products/ services offered further, Businesses/Industries with high AML Risk. For example, dealers in high value or precious goods like bullion dealers, casinos and other gambling businesses, arms & ammunition manufacturers and dealers
- xi. Presence of PEP (Politically Exposed Person)
- xii. Company's activities involve extensive import/export activities, delivery channel used for delivery of products/services.
- xiii. Types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc.
- xiv. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. Further, the risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

C. Customer Identification and Due Diligence Procedures

Part 1: Customer Identification Procedure

An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP shall at all time be in consonance with PML Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

- Verify the identity of any Person transacting with the Company to the extent best possible;
- Maintain records of the information used to verify a customer's identity, including name, address and other identifying information; and
- Consult sanctions lists/ FATF statements of known or suspected terrorists:

1.1 Customer identification means identifying the Customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of every new Customer, whether regular or occasional, and the purpose of the intended nature of business relationship.

1.2 The Customer Identification Procedure (CIP) to be carried out at different stages i.e.



- i. while establishing a business relationship;
 - ii. creating an account-based relationship;
 - iii. carrying out a financial transaction or carrying out any international money transfer operations for a person who is not an account holder of the Company;
 - iv. when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data;
 - v. Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
- 1.3 For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on customer due diligence done by a third party or in house, subject to the following conditions:
- a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
 - b) The Company has taken adequate steps to ensure that the copies of identification data and other relevant documentation relating to the CDD requirements upon request from such third party shall be made available without delay.
 - c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
 - d) The third party shall not be based in a country or jurisdiction assessed as high risk.
 - e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

Part 2: Customer Due Diligence (CDD) Procedure

- CDD for Individual Customers

KAFL, while establishing an account-based relationship or while dealing with an individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity, shall obtain from an individual-

1. Aadhaar number where the individual is desirous of receiving any benefit or subsidy under any scheme or the proof of possession of Aadhaar number or any OVD or the equivalent e-document thereof containing the details of his identity and address where offline verification cannot be carried out;
2. PAN or Form No. 60;
3. the KYC Identifier with an explicit consent to download records from CKYCR; and
4. Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-document thereof.

Provided that –

- i) Where Aadhaar is submitted, the Aadhaar number authentication will be done using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, which is different from the address as per the identity information available in the Central Identities Data Repository, the Company shall obtain a self-declaration to that effect.
- ii) Where proof of possession of Aadhaar is submitted and offline verification can be carried out, the Company shall carry out offline verification.



- iii) Where an equivalent e-document of any OVD is submitted, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I of RBI's Master Direction on KYC.
- iv) Where any OVD or proof of possession of Aadhaar number is submitted and offline verification cannot be carried out, the Company shall carry out verification through digital KYC and be guided by Annex I of RBI's Master Direction on KYC.
- v) Where KYC Identifier is taken Company shall retrieve the KYC records online from the CKYCR in accordance with Section 56 of RBI Master Directions on KYC, 2016.

In case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit under any scheme due to reasons like illness or similar causes as defined by RBI, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD to be done by authorized official only and such exception handling shall also be a part of the concurrent audit and a database is required to be created for such cases.

KAFL shall further ensure that:

1. The customer submitting Aadhaar redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required;
2. Biometric based e-KYC authentication can be done by bank official/ business correspondents/ business facilitators;

The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 & its regulations;

- Non-face-to-face Customers

- i) Non-face-to-face onboarding facilitates the Company to establish business and account bases relationships with the Customer without meeting the Customer physically or through V-CIP. Such onboarding is done through the use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. However, the Company shall undertake the following Enhanced CDD measures while undertaking such onboarding:
 - a. The Company may provide V-CIP process (as applicable under CIP of face-to-face Customers) as the first option to the such Customer for remote onboarding;
 - b. Transactions shall be permitted only from the mobile number used for account opening, and alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc.; further, any requests for change of registered mobile number shall be dealt as per the Board approved policy.
 - c. Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
 - d. The Company shall obtain PAN from such Customers and the same shall be verified from the verification facility of the issuing authority.
 - e. First transaction in such accounts shall be a credit from existing KYC-complied bank account of the Customer.
 - f. Such Customers shall be categorized as high-risk Customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the Customer is verified in face-to-face manner or through V-CIP.



- ii) The Accounts of Non-face-to-face Customers may also be opened using Aadhaar OTP based e-KYC, subject to the following conditions:
- a. Explicit Consent shall be obtained from the Customer for authentication through OTP.
 - b. The transaction alerts, OTP, etc., shall be sent only to the mobile number of the Customer registered with Aadhaar. Any requests for change of registered mobile number shall be dealt as per the Board approved policy in this regard.
 - c. Only term loans with an aggregate amount not exceeding rupees sixty thousand in a year shall be sanctioned.
 - d. Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless the CDD or V-CIP as per this Policy is carried out. If Aadhaar details are used under the V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
 - e. If the CDD procedure are not completed within a year of opening of such account, no further debits shall be allowed.
 - f. A declaration shall be obtained from the Customer to the effect that no other account has been opened nor will be opened using OTP based KYC in Non-face-to-face mode with any other financial institution.
 - g. The Company shall clearly indicate that the account(s) are opened using OTP based e-KYC while uploading KYC information to CKYCR,
 - h. No accounts shall be opened based of KYC information, if the Customer has opened an account with another institution with OTP based e-KYC procedure in non-face-to-face mode.
 - i. The Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

• Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs):

In case a person who desires to open an account is not able to produce documents, as specified in Part 2 (a), the Company may, at its discretion, open accounts subject to the following conditions:

- i. The Company shall obtain a self-attested photograph from the Customer.
- ii. The Designated Officer shall certify under his signature that the Customer has affixed his signature or thumb impression in his presence.
- iii. The account shall remain operational initially for a period of twelve months, within which CDD as per Part 2 and Part 3 shall be carried out.
- iv. The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
- v. The Customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case above mentioned part 2(c)(iv) is violated.
- vi. The Customer shall be notified when the total credit in a year reaches rupees eighty thousand, that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the credit in all the accounts taken together exceeds the limits prescribed in part 2(c)(iv) above.

• CDD Measures for Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out as per documents mentioned in the Annexure in this regard;

• CDD Measures for Legal Entities

In case of opening of account in the name of legal entities such as company, partnership firm, unincorporated association or body of individuals or juridical persons (not specifically covered in the earlier part), such as



societies, universities and local bodies like village panchayats. CDD shall be carried out as per documents mentioned in Annexure in this regard;

- Identification of Beneficial Owner

In case of opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps shall be taken to verify his/her identity, as envisaged under the PML Rules. However, where the Customer or the owner of the controlling interest is a company listed on a stock exchange in India, 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.

- Establishing account-based relationship through the Professional Intermediaries:

The Company shall ensure while establishing an account-based relationship through the professional intermediaries of a Customer, that:

- i. CIP of the Customer, on whose behalf the transactions are sought to be done or an account is sought to be opened by such professional intermediaries, shall be undertaken as per the Policy.
- ii. The Company may hold 'pooled' accounts managed by professional intermediaries on behalf of such Customers, including without limitation any mutual funds, pension funds or other types of funds.
- iii. In case such professional intermediaries are bound by any confidentiality obligation that prohibits disclosure of the Customer's details, the account shall not be opened.
- iv. All the Beneficial Owners shall be identified where funds held by the intermediaries are not co-mingled with respect to their account/relationship with the Company, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled with respect to their accounts/relationship with the Company, the RE shall look for the beneficial owners.
- v. The ultimate responsibility for undertaking the CDD procedure shall lie with the Company.

- Accounts of Politically Exposed Persons (PEPs):

In case of establishing an account-based relationship with PEPs, the Company shall ensure the following:

- i. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- ii. the identity of the person shall have been verified before accepting the PEP as a Customer;
- iii. the decision to open an account for a PEP is taken at a senior level in accordance with the Part 2 (a).;
- iv. all such accounts are subjected to enhanced monitoring on an on-going basis, as per the Applicable Laws, and as deemed necessary by the Company;
- v. in the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, Company shall ensure that requisite internal approvals are obtained to continue the business relationship;
- vi. The CDD measures including enhanced monitoring on an on-going basis shall be applicable to PEPs.
- vii. These provisions shall be applicable in cases where the PEP is a Beneficial Owner.

Part 3: Video based customer identification process (V-CIP)

The Company may decide to undertake live V-CIP for establishment of an account-based relationship with an individual customer, after obtaining his informed consent. The Company will comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as



other general guidelines on IT risks. The technology infrastructure should be housed in own premises and the V-CIP connection and interaction shall originate from own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. RBI's Master Directions on KYC with respect to V-CIP infrastructure will be taken care of.

In this method customer identification is done with facial recognition and customer due diligence by an authorized official of the Company by undertaking seamless, secure, live, informed -consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP.

Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop / disconnection, fresh session shall be initiated.

The Company may undertake V-CIP to carry out CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Further in case of CDD of a proprietorship firm, Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Part 2(d) above, apart from undertaking CDD of the proprietor.

The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

- a. OTP based Aadhaar e-KYC authentication.
- b. Offline Verification of Aadhaar for identification.
- c. KYC records downloaded from CKYCR, in accordance with using the KYC identifier provided by the customer.
- d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.

The Company shall ensure to redact or blackout the Aadhaar number.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, company shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company will ensure that no incremental risk is added due to this.

The Company, while opting to undertake V-CIP, shall adhere to the minimum standards of V-CIP Infrastructure, V-CIP Procedure, V-CIP Records and Data Management as mentioned in RBI's Master Directions.

CDD measures for Sole Proprietary Firms & other Legal Entities

For opening an account in the name of a sole proprietary firm & other Legal Entities, CDD of the shall be carried out as per documents mentioned in Annexure



Identification of Beneficial Owner

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 shall be taken to verify his/her identity keeping in view the following:

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.

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.

Part 4: Ongoing Due-Diligence

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

The Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

D. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures, to effectuate the objectives of the PML Act. The Company can effectively control and reduce their risk only if it has a grasp over the normal and reasonable activity of the Customer, making it possible for the Company to can identify transactions that fall outside the regular pattern of activity

The Company shall pay special attention to all complex, unusually large transactions, transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer and all unusual patterns which have no apparent economic or visible lawful purpose. For ongoing due diligence.

The extent of monitoring shall be aligned with the risk category of the customer. High risk accounts have to be subjected to more intensified monitoring. 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.

The Company does not accept any deposits. Most of the Company's loans are EMI based loans on all categories of Customers. Hence, the transactions with the Company are purely shall be restricted to the EMI/loan repayable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI/loan payable, the threshold for turnover shall be restricted to the aggregate EMIs, penal charges, Fee and/or other payable year after year. No other transactions what so ever nature other than repayment of loan with interest is carried out by the customer with the Company.

8. KYC PERIODIC UPDATATIONS OF ON-BOARDED CUSTOMERS

8.1 The Company shall follow a risk-based approach for KYC updation, where periodic updation is done:

- i. At least once in two years for high risk individuals and entities.
- ii. At least once in every eight years for medium risk



- iii. At least once in every ten years for low risk individuals and entities
- iv. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC

8.2 Updation / Periodic Updation of KYC for Individual Customers

- i. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-declaration to that effect shall be obtained through the email ID/Mobile no. registered with the Company or letter.
- ii. In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through the email ID/Mobile no. registered with the Company and declared address shall be verified through positive confirmation within two months by means such as address verification letter, contact point verification, deliverables etc.
- iii. Fresh photographs will be required to be obtained from minor customer on becoming major. Fresh CDD & KYC, if required may be carried out.
- iv. Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case, the Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

8.3 Updation/ Periodic Updation of KYC for Customers other than individuals:

In case of Legal entities, if there is no change in KYC then a self-declaration through the email ID/Mobile no. registered with the Company and/ or digital channels, letters etc. to such effect will suffice. The Company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible. In case of change in KYC information a fresh CDD & KYC, as applicable to such Legal Entity, shall be carried out.

8.4 Additional Measures:

- The Company will ensure regularly that KYC documents are available with customers as per current CDD standards & in case the validity of CDD documents as available with the Company has expired, then the Company shall undertake the fresh KYC process as applicable to the new on-boarding customer.
- Customer's PAN details, if available with the Company, is to be verified from the database of the issuing authority at the time of periodic updation of KYC. If the PAN or an equivalent document is not available with the Company, or the Customer fails to submit such document within the time as required by the Company, the account of the Customer shall be temporarily ceased until the the Customer ensures such compliance. In case a Customer does not wish to submit his PAN or an equivalent thereof, his account shall be closed, and all obligation in respect thereof shall be settled with such Customer.
- In case there is any change/ update in the documents submitted by the Customer, he shall submit the update of such documents within 30 days of the update to the documents for the purpose of updating the records in the Company's database.
- Company shall ensure to provide acknowledgment with date of having performed KYC updation.
- Physical presence of the clients may, however, not be insisted upon at the time of such periodic updations unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable
- The Company may require more frequent periodicity of KYC updation than the minimum specified periodicity from time to time.
- Fresh photographs will be required to be obtained from minor customer on becoming major.



Further, where client has submitted documents required for the purpose of Due-Diligence, it shall submit to the reporting entity any update on such documents within 30 days of such updation.

9. RECORDS MAINTENANCE & RETENTION

The Company shall have a system of maintaining and preservation of proper record of transactions prescribed under rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as amended from time to time.

The Company shall maintain for at least five years from the date of transaction between the Company and the client, all necessary records (in hard or soft format) of transactions, both domestic or international, which shall permit reconstruction of individual transactions.

The Company shall ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data shall be made available to the competent authorities upon request.

The Company shall register the details of a client, in case of client being a non-profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and a reporting entity has ended or the account has been closed, whichever is later.

10. CUSTOMER EDUCATION, EMPLOYEE HIRING AND EMPLOYEE TRAINING

The Company takes all the necessary steps so as to educate the customer about the KYC requirement through the front-line staffs which are specially trained to deal with customers.

Adequate screening mechanism, including Know Your Employee/ Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.

The staff dealing with / being deployed for KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally.

The Company on an ongoing basis conducts employee training program for all staff and educates them on the elements of AML/KYC/CFT Program. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers.

Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the RE, regulation and related issues shall be ensured.

11. APPOINTMENT OF DESIGNATED DIRECTOR, PRINCIPAL OFFICER AND SENIOR MANAGEMENT

The Company shall have a Board appointed Designated Director and Principal Officer.

A. Designated Director and

Ms. Anita Neerajbhai Chandra, (DIN: 07610732) Whole-time Director & CFO of the Company has been nominated by the Board to act as the Designated Director for the purpose of this Policy.



The Designated Director shall ensure compliance of the obligations imposed under Prevention of Money Laundering Act as amended from time to time.

B. Principal Officer

Mr. Chetankumar Vasantbhai Patel (DIN: 00061443), Director of the Company has been appointed as the Principal Officer for the purpose of this Policy.

The Principal Officer shall be responsible for ensuring compliance, monitoring & reporting of all transactions and sharing of information as required under the PML Act and Rules specified thereunder.

The details and any changes thereof, of the Designated Director and the Principal Officer will be intimated to FIU-IND and to RBI within one month of the appointment.

In no case, the Principal Officer shall be nominated as the Designated Director.

C. Senior Management

For the purpose of this policy, the senior management shall comprises of:

Sr. No.	Name of the Person	Designation
1	Chetankumar Vasantbhai Patel	Director (DIN: 00061443)
2	Anita Neerajbhai Chandra	Whole-time Director & CFO (DIN: 07610732)
3	Mahesh Chandra	Director (DIN: 00061519)
4	Alpesh Bharatbhai Chandra	Director (DIN: 00061548)
5	Aarti Jeetendra Juneja	Independent Director (DIN: 06872059)

12. REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA

All transactions of cash and suspicious as required under PML Act 2002 shall be reported to Financial Intelligence Unit (FIU) from time to time. The Principal Officer specified by the Company shall ensure that such reporting system is in place and shall monitor receipt of the reports.

Further, where the company forms a suspicion of money laundering or terrorist financing, and if it reasonably believes that performing the CDD process will tip-off the customer, the Company shall not pursue the CDD process, and instead file a STR with FIU-IND.

13. REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS COMMUNICATIONS FROM INTERNATIONAL AGENCIES

A. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967

The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, it does not have any account in names of individuals/entities, suspected to having terrorist links, as approved and circulated by United Nations Security Council (UNSC), The details of the two lists are as under;

- (a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & AlQaida Sanctions List is available at: <https://scsanctions.un.org/ohz5jen-al-qaida.html>



- (b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at: <https://scsanctions.un.org/3ppp1en-taliban.html>
- (c) Other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time.

Details of accounts resembling any of the individuals/entities in the list shall be reported to FIU IND and Ministry of Home Affairs as required under UAPA notification dated February 02, 2021 & meticulous compliance shall be ensured.

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.

The KYC policy will apply to Jurisdictions that do not or insufficiently apply the FATF Recommendations in the manner as mentioned in the Master Direction of KYC of RBI.

B. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)

The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India.

The company will not carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

The Company will run check on the given parameters at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

In case of any match in the cases as per given parameters, the Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Company shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the Company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

In case of an order to freeze assets under section 12A is received by the Company from the CNO, the Company will take all such steps to comply with the order without any delay.

For the process of unfreezing of funds, etc., copy of application received from an individual/entity regarding unfreezing shall be forwarded by Company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

The Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the



'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, the Company shall consider – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

14. SECRECY OBLIGATION AND SHARING OF INFORMATION

The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the customer and itself. No details shall be divulged without the express permission of the customer. While considering the requests from Government, Banks or other agencies the Company shall satisfy that the information is not of such nature as would have violated the provisions of laws relating to secrecy of transactions. Notwithstanding to aforesaid, the company may disclose any information where disclosure is under compulsion of law, where there is a duty to the public to disclose, the interest of Company requires such disclosure and where the disclosure is made with the express or implied consent of the Customer.

15. SHARING OF KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

Company shall capture the KYC information for sharing with the CKYCR s, the Company shall capture Customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the Customer, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be, in consonance with the CERSAI guidelines. The Company shall upload KYC records pertaining to accounts of LEs with CKYCR in terms of the provisions of the PMLA Rules, and ensure that the KYC identifier is communicated to the individual/LE upon its generation.

Where a Customer, for the purpose of establishing an account-based relationship, submits a KYC Identifier to a Company, with an explicit consent to download records from CKYCR, the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the Customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless there is a change in the information of the Customer as existing in the records of CKYCR; or the current address of the Customer is required to be verified; or the Company considers it necessary in order to verify the identity or address of the Customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client; or the validity period of documents downloaded from CKYCR has lapsed.

16. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

- (a) The Company shall do 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk as per RBI's guidelines.
- (b) The Company shall also identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including products, practices, services, technologies, new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.
- (c) The risk assessment should be properly documented. While preparing the internal risk assessment, the company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the RBI or any other regulator may specify from time to time.
- (d) The periodicity of risk assessment exercise shall be determined by the Board, based on the outcome of the risk assessment, with minimum review at least annually.



- (e) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.
- (f) The Company shall frame a Board Approved Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard.

The Company shall monitor the implementation of the controls and enhance them if necessary.

17. WIRE TRANSFER

Information requirements for wire transfer, obligation of the Company while ordering, as an intermediary or Beneficiary & other obligation shall be fulfilled as per the provisions of Master Directions on KYC, 2016 as amended from time to time.

Company's responsibility to fulfil record management requirements

Complete originator and beneficiary information relating to wire transfers shall be preserved by the Company if involved in the wire transfer, in accordance with Section 46 of the Master Direction on KYC, 2016 (as amended from time to time).

18. MISCELLANEOUS

- a. Internal audit would evaluate and ensure adherence to the KYC policies and procedures and provide independent evaluation of Company's own policies and procedures, including legal and regulatory requirements. The compliance in this regard would be put up before the Audit Committee of the Board.
- b. Decision-making functions of determining compliance with KYC norms should not be outsourced.
- c. In case of any discrepancy or amendment/change in the RBI Directions with respect to KYC & AML, the effective Directions shall automatically be applied to the Company.

The Company shall follow all other instructions as mentioned under Chapter X of Master Direction of KYC.



Annexure - KYC Documents

Customer Identification Procedure Features to be verified and documents that shall be obtained from customers for undertaking Customer Due Diligence

1. Individuals

Documents to be collected

For Individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity, following documents are required:

- PAN Card/Form 60 (mandatory)
- A certified copy of any other OVD* containing details of his identity and address
 - i. Proof of possession of Aadhaar Card
 - ii. Indian Passport
 - iii. Voter Identity Card
 - iv. Driving License (Booklet Form Not Accepted)
 - v. Job card issued by NREGA duly signed by an officer of the State Government
 - vi. Letter issued by the National Population Register containing details of name and address
- One recent photograph
- The Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962, and
- Such other documents pertaining to the nature of business or financial status

*In case the any of the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be acceptable for the limited purpose of proof of address, provided that the customer shall submit one of the above documents updated with current address within a period of three months of submitting these above documents:

- Utility bill which is not more than 60 days old of any service provider
- property or Municipal tax receipt
- pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
- 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 license agreements with such employers allotting official accommodation

Explanation 1: Where customer submits his Aadhaar number, he may submit it in such form as are issued by the Unique Identification Authority of India.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

2. Sole Proprietorship Firm

Documents to be collected

For opening an account in the name of a sole proprietary firm,



identification information as mentioned under Individuals in respect of the individual (proprietor) shall be obtained mandatorily.

For Proof of the name, address and activity of the concern (Any two of the given documents would suffice. These documents should be in the name of the proprietary concern)*

- Registration certificate including Udyam Registration Certificate issued by Government. (in the case of a registered concern)
- Certificate/license issued by the Municipal authorities under Shop & Establishment Act,
- Sales and income tax returns
- CST/VAT/GSTIN certificate (provisional/final)
- Certificate/registration document issued by Professional Tax authorities/Sales Tax/Service Tax
- License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department, etc. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of the bank account etc.
- The 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 (not older than 60 days)

* If only one document is available, same can be accepted along with a positive contact point verification by the Company FTE at the borrower's place of business

3. Companies

Documents to be collected

For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained mandatorily:

- i. Certificate of incorporation
- ii. Memorandum and Articles of Association.
- iii. Permanent Account Number of the company
- iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
- v. Identification information as mentioned under individuals in respect of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on company's behalf.
- vi. the names of the relevant persons holding senior management position; and
- vii. the registered office and the principal place of its business, if it is different."

4. Partnership Firm

Documents to be collected

For opening an account of a partnership firm, the certified copies of each of the following documents shall be obtained mandatorily:

- i. Registration certificate.
- ii. Partnership deed.
- iii. Permanent Account Number of the partnership firm.
- iv. Identification information as mentioned under individuals in respect of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on company's behalf; and



- v. The names of all the partners and address of the registered office, and the principal place of its business, if it is different.

5. Legal Existence Proof / Address Proof for Trust

Documents to be collected

For opening an account of a Trust, the certified copies of each of the following documents shall be obtained mandatorily:

- i. Registration certificate.
- ii. Trust deed.
- iii. Permanent Account Number or Form No.60 of the trust
- iv. Identification information as mentioned under individuals in respect of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on company's behalf; and
 - the names of the beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust; and
 - list of trustees and documents as are required for individuals for those discharging roles as trustee and authorized to transact on behalf of the trust."

6. Unincorporated Association* or Body of Individuals**

Documents to be collected

For opening an account of an unincorporated association (including Unregistered trusts/partnership firms) or a body of individuals (including societies), certified copies of each of the following documents shall be obtained:

- (a) Resolution of the managing body of such association or body of individuals;
- (b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
- (c) Power of Attorney granted to transact on its behalf;
- (d) Identification information as mentioned under Individuals in respect of the person holding an attorney to transact on its behalf
- (e) such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies

7. Others

Documents to be collected

- a. For opening accounts of Clients purports to act on behalf of juridical person not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats or individual or trust, certified copies of the following documents or the equivalent e-documents thereof shall be obtained: Document showing name of the person authorised to act on behalf of the entity;
- b. Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and
- c. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

= X = X = X =

