KYC & AML POLICY

MAY 12, 2025

SVAKARMA FINANCE PRIVATE LIMITED

Version 1.8

Table of Contents

Background

Svakarma Finance Private Limited [the Company/Svakarma] is engaged in the business of lending to micro, small and medium enterprises (MSMEs) in sectors such as manufacturing, retail trading, food / agriculture and allied services, textiles, rural livelihoods, water & sanitation, etc.

Svakarma offers financing solutions that closely follow the cash flow cycle of our customer's business through an efficient product delivery model coupled with a branch presence in close proximity with the MSME clusters. The ultimate target beneficiary of Svakarma is the underserved participants / consumers in the focus sectors where our involvement **will make a measurable positive impact.**

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

This policy shall be applicable for all group companies of Svakarma for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003).

Accordingly, in compliance with the Master Directions/Guidelines issued by RBI from time to time, the KYC & AML policy of the Company as approved by the Board of Directors of the Company is as given below. This policy is applicable to all categories of products and services offered by the Company.

Below is the list of Senior Management persons who will be responsible for implementation of the Policy:

1. Kalpana Iyer - Managing Director
2. Meenal Jai Singh – Chief Partnerships Officer & Principal Officer
3. Suresh Kulkarni – Chief Risk Officer
4. Taposh Sen – Chief Operating Officer

Objective:

Objective of this Policy is to prevent Svakarma being used, intentionally or unintentionally by criminal elements for money laundering activities. The Policy also mandates making reasonable efforts to determine the true 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, the main objective of this policy is to enable the Company to have positive identification of its customers.

Definition of a Customer

For the purpose of KYC policy, a 'Customer' may be defined as an entity which is engaged in a financial transaction or activity with the Company. The definition also includes any other person / entity on whose

behalf the said transaction or activity is being conducted as well as normally non active parties to such transactions like the co-borrowers and guarantors.

Customer Acceptance Policy (CAP)

The Company shall follow the following norms while accepting and dealing with its customers.

Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable the categorization of the customers into low, medium and high risk.

1. Svakarma will through a detailed Personal Discussion (PD) process collect information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile, the Company will seek only such information from the customer that is relevant to the risk categorisation and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose.
2. The adoption of customer due diligence & acceptance policy, as well as its implementation should not be so restrictive as to result in denial of financial services to the general public, especially those, who are financially or socially disadvantaged.
3. The Company shall carry out full-scale customer due diligence (CDD) before opening a loan account. When the true identity of the account holder is not known, the Company shall not enter into any transaction with such an entity.
4. Additional information, where such information requirement has not been specified in the internal KYC Policy of the Company, is obtained with the explicit consent of the customer.
5. Where the Company is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file a Suspicious Transaction Report (STR).
6. Where the Company is taking GST certificate as CDD, the same shall be verified through the search/verification facility provided by the issuing authority.

Customer Identification Procedure (CIP)

Customer identification implies using reliable and independent source of documents, data or information for establishing the identity of the customer; and where the customer is not an individual then the enterprise's identity. This is to ensure that the customer is not a fictitious person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship. An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP, is integrated into the AML (Anti Money Laundering) program for the Company in terms of the Prevention of Money Laundering Act, 2002 (PMLA), and the relevant rules notified there under which contains provisions

requiring the business processes to:

1. Verify the identity of any Person transacting with the Company to the extent reasonable and practicable;
2. Maintain records of the information used to verify a customer's identity, including name, address and other identifying information;
3. Consult lists of known or suspected terrorists or terrorist organizations and available negative customer lists to determine whether a person opening an account or an existing customer appears on any such list. The same may be done through various KYC verification platforms such as world check, RCU checks etc)
4. The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence [EDD] on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

Customer Due Diligence (CDD) requirements

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. The Company shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements:

a) Identification

Unique identification codes will be used to identify all customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers. The Company shall implement procedures to obtain from each Customer, prior to transacting, the following information as may be relevant, to that business:

1. Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems are exactly the same as (and not merely similar to, or a variation of) the customer name that appears on any identifying documentation reviewed in connection with the loan; In case of mismatch in name of the Borrower with the Documents, a Declaration is taken along with the proof such as marriage certificate, bank statement etc.
2. Latest Photograph- Passport size photo of the Customer.
3. Date of birth / Date of incorporation – for individuals / other than individuals (such as a corporation, partnership, or trust);
4. Address (along with documentary proof thereof) – (a) For individuals- residential or business address (b) for other than individuals- the principal place of business, local office, or other physical location;
5. Telephone/Fax number/E-mail ID;
6. Identification number: Valid PAN or Form 60 as per IT Rules 1962; passport number and country of issuance; letter issued by Unique Identification Authority of India containing AADHAAR number passport or any other government issued document evidencing nationality or residence and bearing a

photograph. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government issued documentation certifying the existence of the business or enterprise;

7. Svakarma can obtain KYC Identifier with explicit customer consent to download KYC records from CKYCR, for the purpose of CDD.

For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but business process shall implement procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period of time before/after disbursal of loan.

The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as Annexure-3 to this policy. These are appropriately covered in the credit policy and communicated to the credit approving authorities.

For proprietary concerns, the Company will collect any two documents from the list given in Annexure-3. Only where the Company is satisfied that it is not possible for the customer to furnish two such documents; the Company will have the discretion to accept only one of those documents as activity proof. In such a situation, the Company will record the appropriate reason for accepting one document as identity proof.
In case of existing KYC compliant customers desirous of opening another account, the KYC process will be guided by relevant guidelines specified under **section j) "risk categorization**" of this policy.

b) Verification

The Company as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

1. Verification through documents: These documents may include, but are not limited to documents listed in Annexure-3 that can be accepted as proof of identity and address from customers across various products offered. These documents are appropriately covered in the credit policy. An independent screening of the KYC documents provided by the customer for its authenticity will also be done through specialized vendors.
   For customers operating under trust / nominee or fiduciary accounts, in addition to the documents as defined under Annexure -3, some additional checks are defined in Annexure 2. The customer verification processes will also be covered in detail in the credit policy.
2. Verification through non-documentary methods: These methods may include, but are not limited to:
   I. Contacting or visiting the customer;
   II. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a bureau / reporting agency, public database, and / or other source;
   III. Checking references with other financial institutions; suppliers and buyers of the prospective customer.

IV. Obtaining a financial statement.

Where appropriate, the business process should implement additional verification procedures. Such verification procedures will be applicable where :

I. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
II. The Svakarma representative is not familiar with the documents presented;
III. Where it is determined that identity verification is not possible through the submitted set of customer documents and
IV. If the business process cannot verify the identity of a non-individual entity, it may be necessary to obtain information about persons with authority or control over such an entity (including authorized signatories) in order to verify the customer entity's identity.

Where a low risk customer (as defined under **section j) "risk categorization**" of this policy) expresses inability to complete the documentation requirements on account of any reason that the Company considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the Company may complete the process for identity verification within six months from the date of establishment of the relationship.

c) Resolution of Discrepancies

Each business process shall document & implement procedures to resolve information discrepancies and to decline or cease to do business with a customer where it cannot form a reasonable belief that it knows the true identity of such customer and / or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

d) Reporting

The Company shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions **greater than Rs.1 lakh**, (excluding loan closure payments) whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

I. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
II. Appears to be made in circumstances of unusual or unjustified complexity; or
III. Appears to have no economic rationale or bonafide purpose or
IV. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
V. Where the transactions are abandoned by customers on being asked to give some details or to provide documents

Further, the Principal officer shall furnish information of the above-mentioned transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

In addition to communicating to the FIU-IND, the Company shall communicate the name, designation,

address and contact details of Designated Director and Principal Officer to the Reserve Bank.

Provided that where the Principal officer, has reason to believe that a single cash transaction or series of cash transactions integrally connected to each other are valued at greater than or **Rs.1 lakhs** (on cumulative monthly aggregate of basis) with a specific purpose of defeating the provisions of the PMLA regulations, principal officer shall furnish information in respect of such transactions to the Director – FIU within the prescribed time.

e) Records Retention

The Company shall document and implement appropriate procedures to retain records of KYC due diligence and anti money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

Transactions for which records need to be maintained for a period of seven (7) years:

I. All cash transactions of the value of more than Rs.1 lakhs or its equivalent in foreign currency.
II. All series of cash transactions integrally connected to each other that have been individually valued below Rs.1 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs 1 lakhs or its equivalent in foreign currency.
III. All cash transactions where forged or counterfeit currency notes or bank notes have been used and/or where any forgery of a valuable security has taken place.
IV. All suspicious transactions whether or not made in cash.

Information to be preserved: The information required to be preserved with respect to the above transactions is the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

Periodicity of retention: The following records shall be retained for a minimum period of ten years after the related customer account is closed

I. The customer identification information and residence identification information including the documentary evidence thereof
II. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity
III. Further, a description of the methods used to verify customer identity as well as a description of the resolution when discrepancies were found, shall be maintained for a period of at least Ten (10) years after such record was created.

The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

f) CIP Notice

The Company shall implement procedures to ensure that customers are given adequate notice when the Company requests information / takes actions towards verifying their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to account opening.

g) Existing Customer

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

h) Enhanced Due Diligence [EDD]

The Company is primarily engaged in lending to micro, small and medium enterprises. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The existing credit policy of the Company in respect of its businesses ensure that the Company is not transacting with such **high-risk customers/ restricted profiles**. The Company shall conduct EDD in connection with all customers or accounts that are deemed to be "potential high risk" and are determined to warrant enhanced scrutiny. Each business process shall establish appropriate standards, methodology and procedures for conducting EDD, which shall involve additional steps beyond what is required by standard KYC due diligence. EDD shall be coordinated and performed by the Company, who may engage appropriate outside investigative services or consult appropriate third party databases when necessary. As a precautionary measure, Svakarma shall conduct dedupe for all the customers on global AML & CTF database like Worldcheck or any other similar software. Each business process shall establish procedures designed to refuse or discontinue customer relationships when the Company cannot adequately complete necessary EDD on the said customer. These procedures will also apply when the information received is deemed to have a significant adverse impact on the Company's reputational risk.

The Company shall verify the current address through positive confirmation before allowing operations in the account. PAN shall be obtained from the customer and shall be verified.

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, etc.

The following are the indicative list where the risk perception of a customer may be considered higher:

I. Customers requesting for frequent change of address/contact details
II. Sudden change in the loan account activity of the customers like frequent excess cash payments.

i) Reliance on third party due diligence

The Company shall, on a need basis, use the services of a third party for due diligence. While using the services of the third party, the Company shall ensure

I. Records or the information of the customer due diligence carried out by the third party is obtained from the third party as per the terms of Service Level Agreement (SLA).
II. Adequate steps are taken by the Company to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
III. 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.

IV. The third party shall not be based in a country or jurisdiction assessed as high risk.

V. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, shall be with the Company.

j) Risk categorization

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out at least once in 6 months. All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization.

Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. 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.

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Since Svakarma is into giving term loans to micro enterprises the due diligence done at the time of opening a loan account (detailed earlier in the policy) will be deemed adequate for the tenor of the loan facility. A fresh due diligence will be done if the customer approaches for another loan facility. For SME customers a mid term review will be done.

In case of a change in address, the customer will notify the company for the change in address and provide the necessary documentary proof and the company will update its records.

An indicative categorization for the guidance of businesses is provided in Annexure 1.

Each business process adopts the risk categorization in their respective **credit appraisal memo** subject to confirmation by compliance based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc.

k) If the Risk Manager believes that the customer needs to be re-categorized into a different risk band, then he may do so by **providing** a justification for the same and getting the approval of the Risk/Business Head.

l) Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity.

However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns that have no apparent economic or visible lawful purpose. Given that the segment the Company is active in is low risk and the facilities offered are term facilities, not in the nature of current or checking accounts and also that its not in the business that involves funds transfer, remittances or cross border transactions, the inherent risk is low and the need for monitoring therefore is minimal.

The Company in due course shall put in place an appropriate software application / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

m) Risk Management

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function also provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The compliance report is put up before the Board on quarterly intervals.

n) Sharing KYC information with Central KYC Records Registry (CKYCR)

Svakarma shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC guidelines prepared for 'individuals' and 'Legal Entities' as the case may be.

o) Customer Education

The Company may regularly educate the customer of the objectives of the KYC program. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joinees on the elements of KYC, AML & CFT through training programs/e-mail.

p) Applicability of branches and subsidiaries outside India:

The Company does not have any branches or subsidiaries outside India at present..

.

q) Appointment of designated Director or Principal Officer:

Kalpana Iyer, Managing Director, shall be the Designated Director, responsible for ensuring overall compliance as required under PMLA Act and the Rules. **Meenal Jai Singh, Chief Partnerships Officer** shall be designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.

Updation/Periodic Updation of KYC

a) 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 from the date of opening of the account / last KYC updation.

Requirements/obligations under International Agreements Communications from International Agencies

a) The UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, shall be verified on a daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.
.

b) Instructions for compliance with the Order dated January 30, 2023, titled - **"Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)"**, issued by the Ministry of Finance, Government of India, have been inserted in Section 52 stipulates detailed requirements and actions to be taken by the stakeholders for freezing / unfreezing of accounts, financial assets, etc., of individuals / entities designated under the list as specified under Section 12A of the WMD Act, 2005. Following additional requirements have been added.

i. In accordance with paragraph 3 of the aforementioned Order, Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
ii. Further, Company shall run a 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.
iii. In case of match in the above cases, Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic Companyources 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.
It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.
iv. Company may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
v. 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, Company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
vi. In case an order to freeze assets under Section 12A is received by the Company from the CNO, Company shall, without delay, take necessary action to comply with the Order.
vii. The process of unfreezing of funds, etc., shall be carried out as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by the 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.

- :
  "In addition to the above, REs shall take into account – (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."
- Vide Section 52, REs have been mandated that they 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 by way 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.

- **Introduction of new technologies**
  The Company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Accordingly, Company shall undertake the risk assessments prior to the launch or use of such products, practices, services and technologies; and take appropriate measures to manage and mitigate the risks.

- **Account opening using Aadhar OTP based e-KYC in non-face-to-face mode:**
  Currently, the Company is not doing non face-to-face customer onboarding.

Annexure-1

Indicative List for risk categorization

Low Risk Category

Individuals and entities (other than high net worth) whose identities and sources of wealth can be easily identified and transactions in whose accounts conform by and large to the known profile, shall be categorized as low risk. Illustrative examples are:

I. Salaried employees whose salary structure is well-defined
II. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
III. Government departments and Government-owned companies
IV. Statutory bodies & Regulators.

Medium & High-Risk Category

Customers that are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples of medium risk category customers are:

I. Non-Resident customers
II. High Net worth Individuals (individuals with taxable annual income greater than 1 Cr)
III. Trust, charities, NGO's and Organization receiving donations
IV. Companies having close family shareholding or beneficial ownership
V. Firms with 'sleeping partners'

Illustrative examples of high-risk category customers are:

I. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
II. Non face-to-face customers
III. Those with dubious reputation as per public information available
IV. Accounts of bullion dealers and jewelers.

Annexure-2

Customer Identification requirements for Trust/Nominee or Fiduciary Accounts

In the case of any application from trust/nominee or fiduciary accounts, the Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

In case of any doubt about the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons, on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. Company shall take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms

Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who comprise the management.
These requirements may be moderated according to the risk perception e.g. in the case of a public Company.

Client accounts opened by professional intermediaries

The Company shall not entertain sourcing of accounts through professional intermediaries. However, should the Company engage a Business Correspondent to act on its behalf to identify and /or service customers it will ensure that the Business Correspondent adopts the KYC guidelines as specified by the Company.

Accounts of Politically Exposed Persons (PEPs)

Politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain the approval of Risk Head and Business Head to continue the business relationship and subject the account to the KYC due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Accounts of Resident Outside India

The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the information available about the person in the public domain. The decision to transact with the PEP should be taken only by the Head of credit of the respective business supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the contracts of the family members or close relatives of PEPs.

Identity of Beneficial Owner

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership.

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:

I. "Controlling ownership interest" means ownership of or entitlement to more than ten percent (10%) of shares or capital or profits of the Company;

II. "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;

(a) 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 fifteen percent (15%) of capital or profits of the partnership;

(b) 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 percent (15%) of the property or capital or profits of such association or body of individuals;

(c) 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;

(d) 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 percent (10%) 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

(e) where the client 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.

The Company will not do any transactions with non-face-to-face customers.

Annexure-3

KYC Documents for Identification and verification

List of documents required for CIP (Customer Identification Procedure):

Common Documents for all Entities

1. PAN Card or Form 60 as per IT Rules 1962
2. Certificate/license issued by the Municipal authorities under Shops & Establishments Act
3. GST certificate (provisional/final)
4. Certificate/registration document issued by Professional Tax authorities
5. GST returns
6. Registration certificate including Udyam Registration Certificate (URC) issued by the Government
7. 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 duly authenticated / acknowledged by the income tax authorities.
8. Utility bills such as electricity, water, landline telephone bills etc.
9. Rent agreement / Lease deed, property documents.
10. IEC (Importer Exporter Code) issued by the office of DGFT or Licence/certificate of practice issued by any professional body incorporated under a statute.

For Proprietors and individuals

Identity Proof & Address Proof (certified copy of any one of the following documents)

1. Passport
2. Voter's identity Card issued by Election Commission
3. Driving license
4. Job card issued by NREGA duly signed by an officer if the State govt.
5. The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar Number.
6. Ration Card with applicant’s Photo

For Partnership firms

1. Partnership deed (registered if available)
2. The names of all the partners; and
3. Address of the registered office, and the principal place of its business, if it is different.
4. Any officially valid document **(OVD)** identifying the partners and the persons holding the Power of Attorney and their addresses
5. Documents of the person holding an attorney to transact on entity’s behalf
   (a) a certified copy of any **OVD** containing details of his identity and address
   (b) one recent photograph
   (c) the Permanent Account Number or Form No. 60, and
   (d) such other documents pertaining to the nature of business or financial status specified in the KYC policy.

For Corporates

1. Certificate of Incorporation
2. Memorandum and Articles of Association
3. Declaration for Beneficial Ownership, if any
4. The names of the relevant persons holding senior management position
5. The registered office and the principal place of its business, if it is different.
6. Documents of the person holding an attorney to transact on entity's behalf
   (a) a certified copy of any **OVD** containing details of his identity and address
   (b) one recent photograph
   (c) the Permanent Account Number or Form No. 60, and
   (d) such other documents pertaining to the nature of business or financial status specified in the KYC policy.
7. In case the customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If such customers are not registered, the Company shall register the details on the DARPAN Portal.

For Trusts

1. Trust deed
2. The names of the beneficiaries, trustees, settlor and authors of the trust
3. The address of the registered office of the trust; and
4. List of trustees and documents, as specified in Section 16, for those discharging role as trustee and authorised to transact on behalf of the trust.
5. Declaration for Beneficial Ownership, if any
6. Documents of the person holding an attorney to transact on entity's behalf
   (a) a certified copy of any **OVD** containing details of his identity and address
   (b) one recent photograph
   (c) the Permanent Account Number or Form No. 60, and
   (d) such other documents pertaining to the nature of business or financial status specified in the KYC policy.

Note:

All the applicants shall have valid ID proof as prescribed above.

Over and above the KYC identification of the customer as per the process laid in above, in case the customer is residing at an address different from the address mentioned in the proof submitted, the Company shall additionally collect any of the documents listed below for communication/contact address purposes:

1. Latest Utility bills [Electricity bill, telephone bill, postpaid mobile phone bill, piped gas bill, water bill] (Not more than two months old).
2. Bank account statement (Not more than six months old).
3. Registered Lease deed along with utility bill in the name of the landlord.
4. Property or Municipal tax receipt.
5. Pension/ Family Pension orders to retired employees of Government Departments, PSU (if they contain address).
6. 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;

The customer shall submit **OVD** with current address within 3 months of submitting the documents above.

Documentation requirements and other information to be collected in respect of different categories of customers are depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;

Illustrative list of activities that would be construed as suspicious transactions

1. Activities that are not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits shall be construed as suspicious transactions.
2. Any attempt to avoid reporting / record-keeping requirements / provides insufficient / suspicious information
3. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
4. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
5. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
6. Certain Employees of the Company arousing suspicion:
    a. An employee whose lavish lifestyle cannot be supported by his or her salary.
    b. Negligence of employees / willful blindness is reported repeatedly.
7. Some examples of suspicious activities/transactions to be monitored:
    a. Multiple accounts under the same name
    b. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
    c. There are reasonable doubts over the real beneficiary of the loan
    d. Frequent requests for change of address