SINGHI CAPITAL FINANCE PRIVATE LIMITED

Policy on Know Your Customer
&
Anti-Money Laundering Measures

Introduction:

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 a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

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

This policy applies to all categories of products and services the Company offers.

2.Objective:

RBI guidelines aim to prevent NBFCs from being intentionally or unintentionally used by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of the customer's business, the reasonableness of operations in the account about 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 identify its customers.

3.Customer Acceptance Policy:

The Company shall observe the following norms while accepting and dealing with its customers:

No account is opened in an anonymous or fictitious / benami name.

The Company shall carry out full-scale customer due diligence (CDD) before opening an account.

When the applicant's true identity is unknown, or the Company cannot apply appropriate CDD measures, no transaction or account-based relationship will be undertaken with such entity.

The Company shall apply CDD measures at the UCIC level.

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

The customer profile contains mandatory information to be sought for KYC purposes relating to the customer's identity, address, social/financial status, nature of the business activity, information about his client's business and location.

The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing a customer profile, the Company will seek only information from the customer that is relevant to the risk category and is not intrusive.

The customer profile will be confidential, and details contained therein will not be divulged for cross-selling or any other purpose. The Company shall maintain secrecy regarding customer information except where the disclosure is under compulsion of law; there is a duty to the public to disclose, and the disclosure is made with the express or implied consent of the customer.

The Company shall ensure that the customer's identity does not match with any person or entity whose name appears in the sanction lists circulated by RBI from time to time.

The policy's intent is not to deny financial services to the general public, especially those who are financially or socially disadvantaged.

While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denying services to genuine customers.

When the account holder's true identity is unknown, the Company shall file Suspicious Transaction Reporting (STR) as provided below in clause 9.

4. Customer Identification Procedure:

The Company shall undertake the identification of customers before the commencement of an account-based relationship.

Customer identification means identifying the customer and verifying their identity by using a reliable and independent source of documents, data or information to ensure that the customer is not a fictitious/ anonymous/ benami 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 the business relationship.

An effective Customer Identification Program ("CIP") is an integral 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 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 reasonable and practicable;

To maintain records of the information used to verify a customer's identity, including name, address and other identifying information and
To consult sanctions lists/ FATF statements of known or suspected terrorists or terrorist organisations/jurisdictions and countries that do not or insufficiently apply the FATF recommendations as provided to the Company by RBI or any other applicable government

agency to determine whether a person opening an account or an existing customer appears on any such list.

The Company will perform appropriate, specific, and, where necessary, Enhanced Due Diligence on its customers that are 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.

The Company will carry out the 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment 'exercise periodically to identify, assess and take adequate measures to mitigate its money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc.

The internal risk assessment carried out by the Company should be commensurate to its size, geographical presence, and the complexity of activities/structure. It shall apply a Risk-Based Approach for mitigating and managing the identified risks.

Respective businesses shall have standard Operating Procedures for identification, mitigation, controls and strategies for managing the identified risk if any.

The risk assessment processes shall be reviewed periodically to ensure their robustness and effectiveness.

5. Required KYC Due Diligence for all customers:

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company.

Each business process shall design and implement appropriate due diligence standards and procedures given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements.

6. Identification:

A unique identification code shall identify all the customers to identify customers, track the facilities availed, holistically monitor financial transactions and have a better approach to risk profiling of customers.

The customer identification requirement is detailed in annexure II of this policy. Each business process shall implement procedures to obtain from each Customer, before transacting, the following information as may be relevant to that business:

a) Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be precisely the

same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;

b) For individuals - age/date of birth;

For a person other than an individual (such as a corporation, partnership or trust) - date of incorporation;

c) Address including the documentary proof thereof;

For an individual, a residential or business street address;

ii. For a Person other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or different physical location;

d) Telephone/Fax number/E-mail ID;

Identification number:

i) A taxpayer identification number; passport number and country of issuance; proof of possession of Aadhaar number; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard or the unique number or code assigned by the Central KYC Records Registry.

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;

Where a customer submits proof of possession of an Aadhaar number, the Company shall ensure that such customer redacts or blackouts his Aadhaar number before submitting the same to the Company.

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

f) One recent photograph of the individual customer. Fresh photos will be received from the minor customer on becoming a major.

For undertaking CDD, the list of documents accepted as proof of identity and address from various customers across various products offered by the Company is given as annexure III to this policy.

These are appropriately covered in the credit policies of the respective businesses and communicated to the credit-approving authorities.

7. Verification:

Each business process, as a part of the credit policy, will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows 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 proof of customer identity, including verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided, and the associated risks.

i) Verification through documents:
These documents may include but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in annexure - III to this policy.

These are appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

ii) Verification through non-documentary methods:
These methods may include, but are not limited to:

Contacting or visiting a customer;

Independently verifying the customer's identity through the comparison of information provided by the customer with data obtained from a consumer reporting agency, public database, or another source;

Checking references with other financial institutions; or

Obtaining a financial statement.

iii) Offline verification through proof of possession of an Aadhaar number:
The Company may carry out offline customer verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Regulations) if the customer is desirous of undergoing Aadhaar offline verification for identification purposes.

No such offline verification will be performed without obtaining the customer's written consent in the manner prescribed in the Aadhaar Regulations.

The Company shall not collect, use or store an Aadhaar number of its customer for any purpose.

iv) Verification of equivalent e-document:
Where the customer submits an equivalent e-document of any Officially Valid Document (OVD) issued by the issuing authority of such document with its valid digital signature, including documents given to the digital locker account of the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act,

2000 and take a live photo of the customer as specified under digital KYC in RBI regulations.

v) Verification through digital KYC:
The Company may carry out verification by capturing a live photo of the customer and OVD or the proof of possession of an Aadhaar, where offline confirmation cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by the authorised officer of the Company as prescribed in RBI regulations.

vi) Video-based customer identification process (V-CIP):
The Company may undertake live V-CIP to establish an account-based relationship with an individual customer after obtaining his informed consent and adhering to the procedures prescribed in RBI regulations. This process shall be treated as face to face process for customer identification.

8) Resolution of Discrepancies:

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence.

These procedures should include the 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.

9) Reporting:

The business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs.10 lakhs, whether such transactions comprise a single transaction or a series of transactions integrally connected, 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:

a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

b) appears to be made in circumstances of unusual or unjustified complexity; or

c) appears to have no economic rationale or bona fide purpose; or

d) gives rise to a reasonable suspicion that it may involve financing activities relating to terrorism.

e) Where customers abandon the transactions on being asked to give some details or to provide documents

An illustrative list of activities which would be construed as suspicious transactions is given in Annexure IV of this policy.

Further, the Principal officer shall furnish information on the transactions mentioned above to the Director of the Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard, including the electronic filing of reports.
Provided that the Principal officer has reason to believe that a single transaction or series of integrally connected transactions have been valued at greater than Rs.10 lakhs to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

The Company shall not restrict operations in the accounts where a suspicious transaction report (STR) has been filed.

The Company shall keep the furnishing of STR strictly confidential and ensure that there is no tipping off to the customer at any level.

The Company shall upload the KYC information about individuals / legal entities, as applicable from time to time, with Central KYC Records Registry (CKYCR) in terms of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

10. Records Retention:

Each business process 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 keeping records:

a. Transactions for which records need to be maintained:
All cash transactions of more than Rs.10 lakhs or its equivalent in foreign currency.

All cash transactions integrally connected have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such transactions have taken place within a month, and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.

All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.

All suspicious transactions, whether or not made in cash.

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

c. Periodicity of retention:
The following records shall be retained for a minimum period of five years after the business relationship is ended:

i. The customer identification information and residence identification information, including the documentary evidence thereof.

ii. All other necessary records about the transactions could be produced as evidence for prosecuting persons involved in criminal activity.

Further, a description of the methods used to verify customer identity and the resolution of any discrepancies in verification shall be maintained for at least Ten (10) years after the such record was created. The above records shall be maintained in hard or soft format and made available to the competent authorities upon request.

11. Customer CIP Notice:

Each business process shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions to verify their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer can view or is otherwise given such notice before account opening.

12. Existing Customers:

The requirements of the earlier sections do not apply to accounts opened by existing customers, provided that the business process has previously verified the customer's identity and the business process has a reasonable belief that it knows the customer's true identity. 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.

13. Enhanced Due Diligence:

The Company is primarily engaged in retail finance. It does not deal with such a category of customers who could pose a potentially high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny.

The Company shall conduct Enhanced Due Diligence with all customers or accounts determined to pose a potentially high risk and warrant enhanced scrutiny.

Each business process in its credit policy shall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting proper additional due diligence or investigative actions beyond what is required by standard KYC due diligence.

Enhanced Due Diligence shall be coordinated and performed by the Company, which may engage outside investigative services or consult appropriate vendor-sold databases when necessary.

Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

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

Customers requesting a frequent changes of address/contact details

Sudden change in the loan account activity of the customer

Frequent closure and opening of loan accounts by the customers

Enhanced due diligence may be like keeping the account monitored closely for a re-categorisation of risk, updating new KYC documents, field investigation or customer visits which shall form part of the credit policies of the businesses.

14) Reliance on third-party due diligence:

To identify and verify the identity of customers at the time of commencement of an account-based relationship, the Company may rely on a third party; subject to the conditions that-

a) the Company obtains records or information of such customer due diligence carried out by the third party within two days from the third party or Central KYC Records Registry;

b) the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client's due diligence requirements will be made available from the third party upon request without delay;

c) the Company is satisfied that such third party is regulated, supervised or monitored for and has measures in place for compliance with client due diligence and record-keeping requirements in line with the needs and obligations under the Act;

d) the third party is not based in a country or jurisdiction assessed as high risk; and

e) the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

15. Risk Categorisation:

The Company shall put in place a periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer.

Such review of risk categorisation of customers will be carried out at a periodicity of not less than once in six months.

The Company shall have a system in place for periodical updation of customer identification data after the account is opened. The entire KYC exercise will be done at a periodicity not less than once in ten years in the case of low-risk category customers, not less than once in eight years in the case of medium-risk category customers and not less than once in two years in the case of high-risk category customers.

Low-risk category customers need not submit fresh proofs of identity and address at the time of periodic updation in case of no change in status concerning their identities and addresses.

A self-certification by the customer to that effect shall suffice in such cases. In case of a change of address of such 'low risk 'customers, they can forward a certified copy of proof of address by mail/post.

If any existing customer fails to submit PAN or equivalent e-document or Form No.60, the Company shall temporarily cease operations in the account until the customer submits the same. To cease the operation in the account, only credits shall be allowed.

However, for customers who cannot provide PAN or equivalent e-document or Form No.60 owing to injury, illness or infirmity on account of old age or such like causes, the Company will continue operation of accounts for such customers subject to enhanced monitoring of the accounts.

All the customers under different product categories are categorised into low, medium and high risk based on their profile. The Credit manager, while appraising the transaction and rendering his approval, will prepare the customer profile based on risk categorisation.

An indicative categorisation for the guidance of businesses is provided in Annexure - I.

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

Where businesses believe that a particular customer falling under a category mentioned below is, in their judgement, falling in a different category, they may categorise the customer so so long as appropriate justification is provided in the customer file.

16) 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 understands the normal and reasonable activity of the customer so that it can identify 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, huge transactions and all unusual patterns with no apparent economic or visible legitimate purpose. High-risk accounts have to be subjected to intensified monitoring.

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

17) Risk Management:

The Company has established appropriate procedures to implement KYC guidelines effectively. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

The company's internal audit and compliance functions evaluate and ensure adherence to the KYC policies and procedures.

As a general rule, the compliance function also provides an independent evaluation of the company's 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 in this regard is put up before the Audit Committee of the Board on quarterly intervals.

The Company ensures that the decision-making functions of determining compliance with KYC norms are not outsourced.

18) Employee Training:

The Company, on an ongoing basis, educates the front-line staff, the branch staff and the new joiners on the elements of AML / KYC through various training programmes and e-mails.

19) Applicability to branches and subsidiaries outside India:

The above guidelines shall also apply to the branches in India.

20) Appointment of Designated Director / Principal Officer:

Mr Hargovind Sachdev, Executive Director, will be the designated director responsible for ensuring overall compliance as required under PMLA Act and the Rules.

Mr Sneh Trivedi, CS, is appointed as Principal Officer, who shall be responsible for furnishing information to FIU-IND.

Annexure – I

Low-Risk Category

Indicative list for Risk Categorisation

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions whose accounts conform to the known profile shall be categorised as low risk.

Illustrative examples are:

1. Salaried employees whose salary structure is well-defined

2. People belonging to lower economic strata of society whose accounts show small balances and
low turnover

3. Government departments and Government-owned companies

4. Statutory bodies & Regulators

Medium & High-Risk Category

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

Illustrative examples of medium-risk category customers are:

a) Non Resident customers

b) High Networth Individuals

c) Trust, charities, NGOs and Organizations receiving donations

d) Companies having close family shareholding or beneficial ownership

e) Firms with 'sleeping partners

Illustrative examples of high-risk category customers are:

1. Politically Exposed Persons (PEPs) of Indian/Foreign Origin

2. Non-face-to-face customers

3. Those with dubious reputations as per public information available

4. Accounts of bullion dealers and jewellers

Annexure - II

Customer Identification Requirements

Trust/Nominee or Fiduciary Accounts
In the case of any application from trust/nominee or fiduciary accounts, the Company determines whether the customer acts on behalf of another person as trustee/nominee or any other intermediary.

If in doubt of 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.

The company takes reasonable precautions to verify the trustees' identity and the trust's settlors (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms
The company needs to be vigilant against business entities being used by individuals as a ‘front ’for transactions.

The company should examine the control structure of the entity and identify the natural persons with 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.
Where the transaction is with a professional intermediary who, in turn, is on behalf of a single client, that client must be identified. The Company shall not open accounts with such professional intermediaries bound by client confidentiality that prohibits disclosing the client details to the Company.

Accounts of Politically Exposed Persons (PEPs) resident outside India
Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of State or Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, and important political party officials.

The Company offers products primarily to Indian residents only. If extending any finance to non-residents, the Company 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 businesses supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms shall also be applied to the contracts of the family members or relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP, the approval of the Head of respective businesses shall be obtained 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 non-face-to-face customers
The Company will not do any transactions with non-face-to-face customers.

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 customer and the person on whose behalf the transaction is

being conducted and includes a person who exercises ultimate effective control over a juridical person.

The government of India has since examined the issue and specified the procedure for determining Beneficial Ownership.

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

Explanation:
I. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five per cent of shares or capital or profits of the company;

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

(b) where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more juridical persons, has ownership of/entitlement to more than fifteen per cent of capital or profits of the partnership;

(c) where the customer 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 persons, 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;

(d) 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;

(e) where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the faith, the trustee, the beneficiaries with fifteen 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. In case the customer is acting on behalf of another person as trustee/nominee, the Company shall obtain satisfactory evidence of the identity of the persons on whose behalf they are working; and

(f) 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.

Annexure III

Customer Identification Procedure – KYC documents that may be obtained from customers

Nature of customer List of applicable documents

As per the list provided to the customer.

Note: Notwithstanding the list of documents stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.

Annexure - IV

Illustrative list of activities which would be construed as suspicious transactions

1. Actions not consistent with the customer's business, i.e. accounts with a large volume of credits, whereas the nature of business does not justify such credits.

2. Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient/suspicious information:

3. A customer reluctant to give the required information for a mandatory report must have the report filed or proceed with a transaction after being informed that the report must be filed.

4. Any individual or group that coerces/induces or attempts to drive/induce the Company employee from not filing any report or other forms.

5. An account with several cash transactions below a specified threshold level avoids filing reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts to prevent the threshold limit.

Certain Employees of the Company arousing suspicion:

An employee whose lavish lifestyle cannot be supported by their salary.

Negligence of employees/willful blindness is reported repeatedly.

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

Multiple accounts under the same name

Refuses to furnish details of the source of funds by which initial contribution is made, sources of funds are doubtful etc.;

There are reasonable doubts over the real beneficiary of the loan

Frequent requests for change of address