



**RBSG CAPITAL PRIVATE LIMITED**  
(AutoMony)

**KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML)  
POLICY**

| <b>S. No.</b> | <b>Contents</b>  |
|---------------|--|
| I             | Preamble   |
| II            | Objective  |
| III           | Key Elements   |
|               | A. Customer Acceptance Policy                            |
|               | B. Customer Identification Procedure                     |
|               | C. Monitoring Of Transaction                             |
|               | D. Risk Management                                       |
| IV            | Identification   |
| V             | Verification   |
| VI            | Maintenance of records of transactions & Identity        |
| VII           | Enhanced Due Diligence                                   |
| VIII          | Appointment of Designated Director and Principal Officer |
| IX            | E-KYC  |



## I. Preamble

Reserve Bank of India (RBI) on February 25, 2016 has notified the Know your customer (KYC) Directions, 2016 (**KYC Directions, 2016**), inter alia, directing that every Regulated Entity shall have a Know Your Customer (KYC) Policy duly approved by the Board of Directors. These directions have been issued by the RBI in terms of the provisions of Prevention of Money-Laundering Act, 2002 (**PMLA**) and the Prevention of Money-Laundering (Maintenance of Records) Rules 2005.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of RBSG Capital Private Limited (herein after referred to as 'Company') is approved by the Board of Directors.

This policy is applicable to all categories of services offered by the Company. The above guidelines shall also apply to the branches and any other offices of the Company.

## II. Objective

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines 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.

## III. Key Elements

KYC procedures also enable us to know/understand our customers and their financial dealings better which in turn help them manage their risks prudently. We have framed our KYC policy incorporating the following four key elements:

- Customer Acceptance Policy
- Customer Identification Procedure
- Monitoring of Transaction and
- Risk Management

For the purpose of KYC policy, a "customer" will be defined as:

- Any person or entity connected with a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.
- Other terms not specifically defined here shall have the same meaning as assigned to them under the KYC Directions, 2016 or the PMLA.
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law.



## **A. Customer Acceptance Policy**

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

- No account is opened in anonymous or fictitious/benami name.
- No account is opened where the Company is unable to apply appropriate CDD (Customer Due Diligence) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- No transaction or account based relationship is undertaken without following the CDD procedure.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
- The company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a Company desires to open another account with the same Company, there shall be no need for a fresh CDD exercise.
- CDD Procedure is followed for all the joint account holders, while opening a joint account.
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
- The customer profile contains 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 which is relevant to the risk category 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.
- The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.

## **B. Customer Identification Procedure**

Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information 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.

The Company shall undertake identification of customers in the following cases:

- (a) Commencement of an account-based relationship with the customer.
- (b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

The customer identification will be through an introductory reference from an existing customer with a satisfactorily conducted loan account or a person known to us and on the basis of documents provided by the customer or through staff members knowing the potential customer or any other document for identification and proof of residence.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence 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.

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 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.

### **C. MONITORING OF TRANSACTION:**

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 which have no apparent economic or visible lawful 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 categorization and updated profile of customers.

#### **Illustrative list of activities which is construed as suspicious transactions**

- Activities 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.
- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient /suspicious information:
  - 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.
  - Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
  - 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.
- Certain Employees of the Company arousing suspicion:
  - An employee whose lavish lifestyle cannot be supported by his or her 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 source of funds by which initial contribution is made, sources of funds is doubtful etc;
  - There are reasonable doubts over the real beneficiary of the loan
  - Frequent requests for change of address

#### **D. RISK MANAGEMENT**

Risk categorization of customers shall be undertaken on the basis of various factors, such as nature of business activity of the customer, location of customer and his/its clients, mode of payments, volume of turnover, social / financial status and credit history. The Company may at its discretion identify additional factors that it may wish to utilize for customer acceptance based on risk profile determined by the Company. The Company may categorize its customers into 'High Risk / Medium Risk / Low Risk' according to risk perceived based on its experience and review it from time to time. The Company may devise procedures for creating risk profiles of its existing and new customers and apply various Anti-Money Laundering measures keeping in view the risks involved in a financial transaction or a business relationship. The Company's internal audit and compliance functions shall play an important role in evaluating and ensuring adherence to KYC policies and procedure, including legal and regulatory requirement. The compliance in this regard is being and will continue to be put up before the Audit Committee on a periodical basis.

#### **IV. IDENTIFICATION:**

##### **CDD Procedure:**

The company shall obtain the following information from an individual while establishing an account based relationship with:

##### **A. Individual**

1. Aadhaar Number (where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained. At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication)
2. Permanent Account Number (PAN)
3. Passport
4. Voter's Identity Card
5. Driving License
6. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company.

The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

##### **B. Proprietary Firms**

1. Aadhaar Number (where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than



6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained. At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication)

2. Permanent Account Number (PAN)
3. Registration Certificate
4. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
5. Sales and income tax returns.
6. CST/VAT/ GST certificate (provisional/final).
7. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
8. 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.
9. Utility bills such as electricity, water, and landline telephone bills
10. Telephone/Fax number/E-mail ID;
11. Recent color photograph

In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/activity.

Provided the Company undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

**C. Company**

1. Certificate of incorporation
2. Memorandum and Articles of Association.
3. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
4. Identification information i.e. Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.

**D. Partnership Firms**

1. Registration certificate
2. Partnership deed
3. Identification information i.e. Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.

**E. Trust**

1. Registration certificate
2. Trust deed.
3. Identification information i.e. Aadhaar Card and PAN Card in respect of trustee, managers, officers or employees holding an attorney to transact on its behalf.

**F. Unincorporated association or body of individuals:**

1. Resolution of the managing body of such association or body of individuals
2. Power of attorney granted to him to transact on its behalf
3. An officially valid document in respect of the person holding an attorney to transact on its behalf.
4. Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals



The Company also ensures that all the customers namely applicant, co applicants and guarantor has valid ID proof as prescribed above

1. The Credit Head of Company has the power to approve the following document in lieu of ID and address proof
  - A certificate from the public authority (i.e) Gazette Officer of State or Central Govt./Magistrate/MRO/VRO/Gram Panchayat Sarpanch/notary public.

#### **In lieu of Identity proof**

- Notarized copy of Marriage certificate with the applicant photograph.

#### **In lieu of address proof**

- Rental agreement along with rent receipt and utility bill of the Landlord.
  - In case the customer has a temporary address being a transit arrangement provided by real estate builder – Allotment letter issued by the builder plus permanent address proof
  - In deserving cases where there is no address proof for one of the applicants or guarantors, an affidavit signed by Close Relative (only in case of spouse, parents or children) confirming that the co applicant / guarantor is staying together in the same address.
2. The Credit Head of Company jointly with the concerned Sales Head has further delegated the approval powers to accept the above documents to credit managers, as they may deem fit and necessary, in this regard.
  3. In the event of any genuine reason for non availability of any of the prescribed documents or to approve any deviations for change in the documents prescribed under this policy, the Credit Head jointly with the Sales Head considers approving any other document not stated above based on the product, market requirements and also on the merits of the case.

#### **V. VERIFICATION**

As part of the Credit Policy of the Company, documents and implemented 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. The Company describes the acceptable methods of verification of customer identity, which includes verification through documents or non documentary verification methods that are appropriate 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 by the Company as provided in annexure to this policy. These are appropriately covered in the Credit Policy of the Company.

The Company also accepts physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post is also accepted as an 'Officially Valid Document'.

As per RBI instruction the Company also downloads e-Aadhaar from UIDAI website as an officially valid document subject to the following:

- a) If the prospective customer knows only his / her Aadhaar number, the Company needs to print the prospective customer's e-Aadhaar letter in the company directly from the UIDAI portal; or adopt e-KYC procedure as mentioned below.
- b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the Company prints the prospective customer's e-Aadhaar letter directly from the UIDAI portal; or adopt e-KYC procedure as mentioned below.

**Verification through non-documentary methods:**

Indeed the Company mainly depend upon this method:

1. Contacting or visiting a customer;
2. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
3. Checking references with other financial institutions; or
4. Obtaining a financial statement.

**ii. Additional verification procedures.**

The business process verification procedures of the Company also address the following situations where:

1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The sales executive is not familiar with the documents presented;
3. Where the sales executive is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents; and
4. If the sales executive cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

The Credit Head along with Sales Head, advise the credit managers to make a personal visit to entangle the situation. The Company will not do any transactions with non-face-to-face customers.



## **VI. MAINTENANCE OF RECORDS OF TRANSACTIONS & IDENTITY**

As unlikely as it will be in the Company's case, due to its focus on lower income families, the company has a system of maintaining proper record of transactions prescribed under Rule 3, of the Prevention of Money-Laundering and value of transactions, the procedure and manner of maintaining and verification and maintenance of records of the identity of the clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, as mentioned below:

- all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency
- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh
- 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 and by way of as mentioned in the Rules.

### **Information to be preserved:**

As per the RBI guidelines, the company maintains the following information in respect of transactions referred to in Rule 3

- the nature of the transactions
- the amount of the transaction and the currency in which it was denominated
- the date on which the transaction was conducted;
- the parties to the transaction.

### **Maintenance and Preservation of records:**

The company has a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. The company will maintain for at least five years from the date of cessation of transaction between the company and the customer, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

The company also ensures that records pertaining to the identification of the customer and his / her address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the loan 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 will be made available to the competent authorities upon request.



## VII. ENHANCED DUE DILIGENCE

The company is primarily engaged in MSME finance. 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 policies of the company in respect of its various businesses ensure that the company is not transacting with such high risk customers.

The company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. The company has established appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate 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.

The following are the indicative list where the risk perception of a customer which is considered higher:

- i. Customers requesting for frequent change of address/contact details
- ii. Sudden change in the loan account activity of the customers
- iii. Frequent closure and opening of loan accounts by the customers

### **CIP Notice:**

Enhanced due diligence is in the nature of keeping the account monitored closely for a re-categorisation of risk, updation of fresh KYC documents, field investigation or visit of the customer, etc., which forms part of the credit policies of the businesses.

The Company shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions in order 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 is able to view or is otherwise given such notice prior to account opening.

### **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.

### **Reliance on third party due diligence:**

The company shall not rely on third party due diligence.



**VIII. APPOINTMENT OF DESIGNATED DIRECTOR / PRINCIPAL OFFICER**

Mr. Rishab Bafna, Director of the Company will be the Designated Director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules.

Mr. Shirang Date is designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.

As per the RBI guidelines, the Principal Officer is located at our corporate office and is responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He maintains a close liaison with enforcement agencies, other NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

**IX. EKYC**

E-KYC authentication facility as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e- KYC data along with other technical details related to the authentication transaction

.....

