# Snowball KYC Policy

Snowball and related entities partner with Sumsub.com for our KYC requirements.

The Company shall follow customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. The policy is based on Anti Money Laundering (AML) standards.

1. Information collected from the customer for the purpose of opening of account shall be kept confidential and the Company shall not divulge any details thereof for cross selling or any other purposes. Information sought from the customer shall be relevant to the perceived risk, shall not be intrusive, and shall be in conformity with the guidelines issued by Snowball from time to time. Any other information from the customer shall be sought separately with his/ her/ its consent and after opening the account.

2. The objective of the KYC policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/ understand its customers and their financial dealings better, which in turn help the Company to manage its risks prudently. The Company has framed its KYC policy incorporating the following four key elements:

(i) Customer Acceptance Policy;
(ii) Customer Identification Procedures;
(iii) Monitoring of Transactions/ On-going Due Diligence; and
(iv) Risk Management.

3. For the purpose of the KYC policy:

a) “Beneficial Owner” refers to the natural person(s) who ultimately owns or controls a customer and/ or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

b) “Customer” means a person that engages in a financial transaction or activity with the Company and includes a person on whose behalf the person that engages in the transaction or activity is acting.

c) “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner using ‘Officially Valid Documents’ as a ‘proof of identity’ and ‘proof of address’.

h) “Politically Exposed Persons (PEPs)” are:

(i) individuals who are or have been entrusted with prominent public functions domestically or by a foreign country, e.g., Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;

(ii) international organization PEPs who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors and members of the board or equivalent functions, and
(iii) family members related to PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership; and
(v) close associates are individuals who are closely connected to a PEP, either socially or professionally.

j) "Principal Officer" means an officer designated by the Company.

4. Customer Acceptance Policy (CAP):

The criteria for acceptance of customers are as follows:

(i) No account shall be opened in anonymous or fictitious/ benami name(s);
(ii) No transaction or account based relationship will be undertaken without following the Customer Due Diligence (CDD) procedure.

a. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updates as specified, should be obtained.
b. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
c. CDD procedure is followed for all the joint account holders while opening a Joint Account.

(iii) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity;

(iv) Parameters of risk assessment in terms of the customers' identity, social/ financial status, nature of business activity, information about the clients' business and their locations, etc. have been defined to enable categorization of customers into low, medium and high risk.

While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities or other entities may also be factored in documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Snowball from time to time;

(v) The Company shall not open an account where it is unable to apply appropriate CDD measures, i.e., the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example,

decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
(vi) Before opening a new account necessary screening will be performed so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or whose name appears in the lists circulated by RBI/ SEBI/ NHB/ IRDA, United Nations Security Council (UNSC), OFAC, as per section 51A of the Unlawful Activities (Prevention) Act, 1967, watch list by Interpol, etc. These are done using the list/ information/ databases available on World-check, Watch-out Investors, website of OFAC, UNSCR (as mentioned below) or such other information sources/tools.

The Company shall prepare a profile for each new customer based on risk categorization, as provided subsequently in this policy. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

(vii) For the purpose of risk categorisation, individuals (other than High Net Worth individuals) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk.

Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.
Customers that are likely to pose a higher than average risk to the company shall be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and client profile etc. The Company shall apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive ‘due diligence’ for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring enhanced due diligence shall include (a) trusts, charities, NGOs and organizations receiving donations, (c) companies having close family shareholding or beneficial ownership, (d) firms with 'sleeping partners', (e) Politically Exposed Persons, (f) those with dubious reputation as per public information available, etc.
The adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

**5. Customer Identification Procedure (CIP)**

Customer Identification Procedure to be carried out at different stages as under:

- Commencement of an account-based relationship with the customer;
- When the Company has a doubt about the authenticity or adequacy of the customer identification data obtained by the Company. Customer identification means identifying the customer and verifying his/ her/ its identity by using reliable, independent source documents, data or information; and

- Carrying out a financial transaction.

a) The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the Company should be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer, in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.). For customers that are natural persons, the Company shall obtain sufficient identification data to verify the identity of the customer, his/ her address/ location, and also his/ her recent photograph. For customers that are legal persons or entities, the Company shall (i) verify the legal status of the legal person/ entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person; and (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

If the Company accepts such accounts in terms of the Customer Acceptance Policy, the Company shall take reasonable measures to identify the beneficial owner(s) and verify his/ her/ their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

Our list of the nature and type of documents/information that shall be relied upon for customer identification is;

- passport or national ID number, and country of issuance;
- date of birth;
- residential or business address;
- phone number;
- email address;
- sample signatures;
- other financial information, such as the purpose for opening a trading account, source of funds, etc.

b) Introduction shall not be sought while opening accounts.
c) The Company shall not ask the customer to furnish an additional OVD, if the OVD submitted by the customer for KYC contains both proof of identity and proof of address. Further, the customer shall not be required to furnish separate proof of address for permanent and current addresses, if these are different. The Company shall obtain a declaration from the customer about her/ his local address on which all correspondence will be made by the Company, in the event the proof of address furnished by the customer is the address where the customer is currently residing.

The Company shall allot Unique Customer Identification Code (UCIC) to all their customers while entering into any new relationships.

**6. Monitoring of Transactions/ On-going Due Diligence:**

a) The Company shall pay special attention to all large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
b) The Company shall prescribe threshold limits for specific categories of accounts and pay particular attention to the transactions which exceed prescribed thresholds, based on income and / or net worth of the customer.
c) Currently, no cash transactions are done by the Company, since all disbursements and repayments are made through normal banking channels only. However, should it ever be necessary to operate cash, transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.
d) High-risk accounts shall be subjected to intensify monitoring and enhanced due diligence. The Company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. The Company shall put in place a system of periodical review of risk categorization of accounts, with such periodicity being at least once in 6 (six) months and the need for applying enhanced due diligence measures.
e) The records of transactions in the accounts shall be preserved and maintained as required in terms of section 12 of the PML Act, 2002. The Company shall report the transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PMLAct, 2002, to the appropriate law enforcement authority.
f) While currently, no cash transactions are undertaken, in the unforeseen event of such transactions taking place, the Company will maintain a proper record of all cash transactions (deposits and withdrawals) of $100 USD and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a fortnightly basis.

**7. Risk Management:**

a) Through this policy, the Board of Directors of the Company is ensuring the formal documentation of its KYC programme. The management will establish appropriate procedures to ensure its effective implementation.
b) The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function would provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The audit machinery shall be staffed adequately with individuals who are well-versed in such policies and procedures. The Internal Auditors shall 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 shall be put up before the Audit Committee of the Board on quarterly intervals.
c) The Company shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC and AML procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new

customers. It is crucial that all those concerned fully understand the rationale behind the KYC policy and implement the same consistently.

**10. Review of KYC for the Existing Accounts:**

a) The Company shall also apply this policy to the existing customers on the basis of materiality and risk. Moreover, transactions in existing accounts shall be continuously monitored and any unusual pattern in the operation of the account shall trigger a review of the CDD measures.
b) The Company shall consider applying monetary limits to such accounts based on the nature and type of the account. All the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'. Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and/ or non-cooperation by the customer, the Company shall consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions shall be taken at a reasonably senior level.
d) The Company shall carry out periodic updation at least once in every 2 years for high risk customers, once in every 8 years for medium risk customers and once in every 10 years for low risk customers, subject to the following conditions:
- Fresh proofs of identity and address shall not be sought at the time of periodic updation, from low risk customers, when there is no change in status of their identities and addresses and a self-certification to that effect is obtained;
- certified copy of the proof of address forwarded by ‘low risk’ customers through mail/ post, etc. in case of change of address shall be acceptable;
- physical presence of low risk customer at the time of periodic updations shall not be insisted upon; and
- time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

**11. Appointment of Principal Officer:**

The Company has appointed a senior management officer designated as the Principal Officer. The Principal Officer shall be located at the head office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, the Company and any other institution, which are involved in the fight against money laundering and combating financing of terrorism.

**12. Record Management:**
In order to maintain, preserve and report the customer account information, with reference to provisions of PML Act and Rules, the Company shall:
1) maintain all necessary records of transactions between the Company and the customer for at least 5 (five) years from the date of transaction;
2) preserve the records pertaining to the identification of the customers and their addresses

obtained while opening the account and during the course of business relationship for at least5 (five) years after the business relationship is ended;
3) make available the identification records and transaction data to the competent authorities upon request;
4) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005;
5) maintain all necessary information in respect of transactions prescribed under PML Rule 3 as to permit reconstruction of individual transaction, including the nature, amount and date of transaction and the parties to the transaction;
6) evolve a system for proper maintenance and preservation of account information in a manner that allows easy and quick retrieval of data whenever required or requested by the competent authorities; and
7) maintain records of identity and address of the customers and records in respect of transactions referred to in PML Rule 3 in hard or soft format.
The Company shall upload the KYC data pertaining to all new individual accounts opened on or after April 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.