KNOW YOUR CUSTOMER (KYC) & PREVENTION OF MONEY LAUNDERING (PMLA) POLICY

SNAPMINT FINANCIAL SERVICES PRIVATE LIMITED

PREAMBLE:

Prevention of Money Laundering Act, enacted by the Parliament in 2002, the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India makes it obligatory for all the Regulated Entities (REs) to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. [1]REs shall take steps to implement the provisions of the aforementioned Act, Rules and Ordinance, including operational instructions issued in pursuance of such amendment(s). Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act ibid, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified. As per the KYC principles, intermediaries have to collect documents known as KYC documents before entering into any transaction with the customers. The KYC process includes making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, nature of customer's business, reasonableness of operations in the account visa-versa customer's business/income profile etc. The KYC requirement is applicable to all categories of customers transacting with any financial intermediary. The Guidelines on 'Know Your Customer' and' Anti-Money Laundering Measures' for Snapmint Financial Services Private Limited, hereinafter mentioned as 'Snapmint' that are to be followed are enlisted in the Policy.

CHAPTER – I

OBJECTIVE:

The objective of KYC/AML policy is to prevent the Companies from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures enable Banks/ Financial Intermediaries to understand their customers and their financial dealings better which in turn help them manage their risks prudently. The KYC process has become the utmost necessity for all financial intermediaries in the era of fast dispersion money-laundering hazard across the globe.

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Snapmint Financial Services Pvt. Ltd. is required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. Snapmint shall take steps to implement provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

SHORT TITLE AND COMMENCEMENT:

1. General:

1.1. These Guidelines shall be called the Guidelines on 'Know Your Customer' & 'Anti-Money Laundering Measures' for Non-Banking Financial Companies.

1.2. These Guidelines shall come into effect on the day they are placed on the official website of the Snapmint Financial Services Pvt. Ltd.

2. Applicability:

The provisions of these Guidelines shall apply to Snapmint regulated by the Reserve Bank of India, except where specifically mentioned otherwise.

3. Definitions:

3.1. In these Guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below: -

3.1.1. "Aadhaar number" means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the' Aadhaar Act';

3.1.2. "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 respectively and amendments thereto;

3.1.3. "Authentication" means the process as defined under sub-section (c) of section 2 of the Aadhaar Act;

3.1.4. Beneficial Owner (BO):

(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 person, has/have a controlling ownership interest or who exercise control through other means.

Explanation - For the purpose of this sub-clause:-

(i). "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the 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.

(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 person, has/have ownership off entitlement to more than 15per 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 person, has/have ownership off entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation- Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(d). Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and are:(other natural person exercising ultimate effective control over; trust. through a chain of control or ownership.

3.1.5. Certified Copy of OVD" - Obtaining a certified copy by regulated entity shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the regulated entity.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

3.1.6. "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) (aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

3.1.7. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

3.1.8. "Officially Valid Document" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address;

Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

    i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
    ii. property or Municipal tax receipt;
    iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
    iv. 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;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

3.1.9. "Offline Verification", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

3.1.10. "Person" has the same meaning as defined in the Act and includes:
a) an individual,

b) a Hindu undivided family,
c) a company,
d) a firm,
e) an association of persons or a body of individuals, whether incorporated or not,
f) every artificial juridical person, not falling within anyone of the above persons (a to e), and
g) any agency, office or branch owned or controlled by any of the above persons (a to f).

3.1.11. "Principal Officer" means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

3.1.12. “Suspicious transaction” means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to not have economic rationale or bona-fide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

3.1.13. "Transaction" means means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- opening of an account;
- deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- the use of a safety deposit box or any other form of safe deposit;
- entering into any fiduciary relationship;
- any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- establishing or creating a legal person or legal arrangement.

3.1.14 “Customer” means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.1.15. "Customer Due Diligence" (CDD) means "Client Due Diligence" means identifying and verifying the customer and the beneficial owner.

3.1.16. "Customer Identification" means undertaking the process of CDD.

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

3.1.18. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR for individuals and legal entities

3.1.19. "Non-face-to-face customers" means customers who open accounts without visiting the branch/ offices of the Snapmint or meeting the officials of Snapmint.

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

3.1.21. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank of India.

3.1.22. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions e.g., Heads of States/ Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

3.2. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the 8Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder and ‘Aadhaar and other Laws (amendment) Ordinance, 2019’, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. **Designated Director:**

A "Designated Director" means a person designated by the Snapmint to ensure overall compliance with the obligations imposed under Chapter IV of the Act and shall be nominated by the Board of the Snapmint.

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

The name, designation and address of the Designated Director, including changes from time to time, shall be communicated to the Director, FIU-IND and also to the Regional Office of Reserve Bank of India.

5. **Principal Officer:**

The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

The name, designation and address of the Principal Officer shall be communicated to the FIU-IND and also to the Regional Office of Reserve Bank of India.

6. **Compliance of KYC policy:**

(a) Snapmint shall ensure compliance with KYC/AML Policy through:

- Specifying as to what constitutes 'Senior Management' for the purpose of KYC compliance.
- Allocation of responsibility for effective implementation of policies and procedures.
- Independent evaluation of the compliance functions of Snapmint's policies and procedures, including legal and regulatory requirements.
- Concurrent/internal audit system to verify the compliance with KYC/ Anti-Money Laundering (AML) policies and procedures.
- Submission of quarterly audit notes and compliance to the Audit Committee.

(b) Snapmint ensures that decision-making functions for determining compliance with KYC norms are not outsourced.

CHAPTER - II

Snapmint Financial Services Pvt. Ltd. has framed a KYC/AML Policy with the following key elements:

a) Customer Acceptance Policy;
b) Risk Management;
c) Customer Identification Procedures (CIP); and
d) Monitoring of Transactions

DEFINITION OF CUSTOMER:

For the purpose of KYC policy, a "Customer" to be defined as:

- A person or entity that maintains an account and/ or has a business relationship with the Company.
- One on whose behalf the account is maintained (i.e. the beneficial owner);
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Company Secretaries, Solicitors etc. as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of a high value demand draft as a single transaction.

CHAPTER - III

CUSTOMER ACCEPTANCE POLICY

Snapmint Financial Services Pvt. Ltd. shall lay down a clear Customer Acceptance Policy with explicit criteria for acceptance of customers. The Customer Acceptance Policy shall ensure that explicit guidelines are in place on the following aspects of customer relationship in the Snapmint:

a) No account to be opened in anonymous or fictitious/ benami name(s)
b) No account is opened where the Snapmint is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
c) No transaction or account-based relationship is undertaken without following the CDD procedure.
d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
e) Optional or additional information, is obtained with the explicit consent of the customer after the account is opened.
f) CDD Procedure is followed for all the joint account holders, while opening a joint account.
g) If an existing KYC compliant customer of Snapmint desires to open another account with us, there shall be no need for a fresh CDD exercise.
h) Circumstances in which, a customer is permitted to act on behalf of another person/ entity, is clearly spelt out.
i) 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 issued by UN Security Council circulated by Reserve Bank of India from time to time.
j) Parameters of risk perception to be clearly defined in terms of the location of customer and his clients and mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into low, medium and high risk
k) 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 Prevention of Money Laundering Act, 2002 (Central Act No. 15 of 2003) (hereinafter referred to as PMLA), rules framed there under and guidelines issued from time to time;

l) Necessary checks before opening a new account 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, etc.

*Implementation of this policy related to customer acceptance, does not result in denial of Snapmint's services to general public especially to those who are financially or socially disadvantaged.

CHAPTER - IV

RISK PROFILE

Snapmint Financial Services Pvt. Ltd. will prepare a profile for each new customer which may contain information relating to the 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 Snapmint. However, while preparing the customer profile, Snapmint will seek only such information from the customer which is relevant 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 purposes.

The Risk categorisation shall be undertaken based on parameters such as customer's identity, social, financial status, nature of business activity, and information about the clients' business and their location 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. Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same may be specified in this Policy. The Recommendations made by the Financial Action Task Force (FATF) on Anti-money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) standards should also be used in risk assessment.

As per KYC policy, for acceptance and identification, Company's Customers shall be categorized based on perceived risk broadly into three categories – A, B & C. Category A includes High Risk Customers, Category B contain Medium Risk Customers while Category C Customers include Low Risk Customers. None of the Customers will be exempted from Company's KYC procedure, irrespective of the status and relationship with Company or its Promoters. The above requirement may be moderated according to the risk perception as explained in Annexure I.

(i) High Risk–(Category A):

High Risk Customers typically includes:

a) Non-Resident Customers;

b) High net worth individuals without an occupation track record of more than 3 years;

c) Trust, charitable organizations, Non-Government Organization (NGO), organizations receiving donations;

d) Companies having close family shareholding or beneficial ownership;

e) Firms with sleeping partners;

f) Politically exposed persons (PEPs) of foreign origin;

g) Person with dubious reputation as per public information available;

(ii) Medium Risk – (Category B):

Medium risk Customers will include:

a) Salaried applicant with variable income/ unstructured income receiving Salary in cheque;

b) Self- employed professionals other than High Net worth individuals.

c) Self-employed customers with no credit history

d) High Net worth individuals with occupation track record of more than 3 years;

(iii) Low Risk-(Category C):

Low Risk individuals (other than high net worth) and entities whose identities and sources of wealth or credit record can be easily identified and all other person not covered under above two categories. Customer carrying low risk may include the following:

a) Salaried employees with well-defined salary structures for over 5 years;
b) Consumers with good credit score – salaried and self employed

c) People working with government owned companies, regulators and statutory bodies, MNC's, rated companies public sector units, public limited companies etc. In the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company will obtain senior management approval in such cases to continue the business relationship with such person, and also undertake enhanced monitoring as indicated and specified in Annexure I;

d) People belonging to lower economic strata of the society whose accounts show small balances and low turnover;

e) People working with Public Sector Units;

f) People working with Private limited companies

The Company shall subject accounts of such customers to intensive due diligence. In the event of an existing customer subsequently becoming a PEP, the Company shall obtain necessary approval of the Senior Management to continue the business relationship with such person and if in the affirmative than the Company to undertake enhanced monitoring at regular period.

CHAPTER - V

CUSTOMER IDENTIFICATION PROCESS

Snapmint Financial Services Pvt. Ltd. will follow clear RBI guidelines on the Customer Identification Procedure to be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when Snapmint has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. Snapmint will 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 relationship. Being satisfied means that Snapmint must 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.). In following cases identification should be done:

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.
c) Selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand.

- For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Snapmint shall at their option, rely on CDD done by a third party, subject to the following conditions:

a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
b) Adequate steps are taken by Snapmint 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.
c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping

requirements in line with the requirements and obligations under the Prevention of Money-Laundering Act.

d) The third party shall not be based in a country or jurisdiction assessed as high risk.
e) The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall rest with the Snapmint.

CHAPTER - VI

CUSTOMER DUE DILIDENCE PROCESS:

Part I - Customer Due Diligence (CDD) Procedure in case of Individuals

1. While undertaking CDD, Snapmint Financial Services Pvt. Ltd. shall obtain the following information from an individual while establishing an account-based relationship with an 'individual' or dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:
   i. a certified copy of any OVD containing details of his identity and address
   ii. one recent photograph
   iii. the Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962, and
   iv. such other documents pertaining to the nature of business or financial status specified by the REs in their KYC policy.

   Snapmint may carry out offline verification of a customer if it is desirous of undergoing Aadhaar offline verification for identification purpose. In cases where successful authentication has been carried out, other OVD and photograph need not be submitted by the customer.

   CDD done in this manner shall invariably be carried out by an official of the Snapmint and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. Snapmint shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Snaapmint and shall be available for supervisory review.

   Explanation 1- Snapmint shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

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

Part- II Accounts of Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, identification information in respect of the individual (proprietor) shall be obtained. In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

a) Registration certificate.
b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
c) Sales and income tax returns.
d) GST certificate (provisional/ final).
e) Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities.
f) lEC (Importer Exporter Code) issued to the proprietary concern by the office of DCFT/Licence/ certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g) 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.
h) Utility bills such as electricity, water, and landline telephone bills.

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

Provided Snapmint 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.

PART III – Account of Legal Entities:

I. For opening an account of a company, one certified copy of each of the following documents shall be obtained:

a) Certificate of incorporation;
b) Memorandum and Articles of Association
c) Permanent Account Number of the company;
d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
e) Documents, as specified in Part I (1), of the person holding an attorney to transact on its behalf

II. Account of Partnership Firm

In order to confirm the correctness of the Legal Name, Address, name of all partners and their addresses and Telephone numbers of the firm and partners given in the account opening form, the following documents may be obtained for verification:

a) Registration certificate, if registered
b) Partnership deed
c) Permanent Account Number of the partnership firm
d) Documents, as specified in Part I (1), of the person holding an attorney to transact on its behalf

III. Accounts of trusts and foundations -

In order to confirm the correctness of the Name of trustees, settlers, beneficiaries and signatories, Names and addresses of the founder, the manager / directors and the beneficiary/ies, Telephone / fax numbers, the following documents may be obtained for verification:

a) Trust Deed
b) Certificate of registration, if registered
c) PAN or Form 60 of the Trust
d) Documents, as specified in Part I (1), of the person holding an attorney to transact on its behalf

IV. Accounts of unincorporated association or a body of individuals:

For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:

a. Resolution of the managing body of such association or body of individuals
b. PAN or Form No. 60 of the association or BOI.
c. Power of attorney granted to him to transact on its behalf
d. Documents, as specified in Part I (1), of the person holding an attorney to transact on its behalf.
e. Such information as may be required by the Snapmint to collectively establish the legal existence of such an association or body of individuals.

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

Explanation: Term 'body of individuals' includes societies.

* Explanation - Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and the term 'body of individuals, includes societies.

V. For opening accounts of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents shall be obtained:

a) Document showing name of the person authorised to act on behalf of the entity;
b) documents, as specified in Part I (1), of the person holding an attorney to transact on its behalf.
c) Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

PART IV– CDD Measures for Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his/her identity shall be undertaken keeping in view the following:

a) 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.

b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

PART V - ENHANCED DUE DILIGNECE MEASURES

1. Accounts of Non-face-to-face customers: Snapmint shall ensure that the first payment is to be affected through the customer's KYC-complied account, for enhanced due diligence of non-face to face customers.

2. Accounts of Politically Exposed Persons (PEPs): Snaapmint shall have the option of establishing a relationship with PEPs provided that:
   a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
   b) the identity of the person shall have been verified before accepting the PEP as a Customer
   c) the decision to open an account for a PEP is taken at a senior level in accordance with the Snapmint's Customer Acceptance Policy;
   d) all such accounts are subjected to enhanced monitoring on an on-going basis;
   e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
   f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

3. Customer's accounts opened by Professional Intermediaries:

Snapmint shall ensure while opening customer's accounts through professional intermediaries, that:

a) Customer shall be identified when client account is opened by a professional intermediary on behalf of a single client.
b) Snapmint shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c) Snapmint shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.
d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Snapmint, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Snapmint, the Company shall look for the beneficial owners.
e) Snapmint shall, at their discretion, rely on the CDD done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
f) The ultimate responsibility for knowing the customer lies with Snapmimt.

CHAPTER - VII

ON-GOING DUE-DILIGENCE:

1. Snapmint shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.
2. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

    a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
    b. Transactions which exceed the thresholds prescribed for specific categories of accounts.
    c. High account turnover inconsistent with the size of the balance maintained.
    d. Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

3. The extent of monitoring shall be aligned with the risk category of the customer.

    Explanation: High risk accounts have to be subjected to more intensified monitoring.

    a. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
    b. The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

    Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

PERIODIC UPDATION:

Periodic KYC updation shall be carried out at least once in every two years for high risk customers, once in every five years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

a) Snapmint shall carry out

   i. CDD, as specified in Part I (1), at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.
   ii. In case of Legal entities, RE shall review the documents sought at the time of opening of account and obtain fresh certified copies.

b) Snapmint may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD / Consent forwarded by the customer through mail/ post, etc., shall be acceptable.

c) EHFL – what is this? shall ensure to provide acknowledgment with date of having performed KYC updation.

d) The time limits prescribed above would apply from the date of opening of the account's last verification of KYC.

CHAPTER VIII - MAINTENANCE OF RECORD OF TRANSACTION

I. The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Snapmint shall,

(a) maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;
(b) 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 least five years after the business relationship is ended;
(c) make available the identification records and transaction data to the competent authorities upon request;
(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

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

(f) evolve 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;
(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

II. MAINTENANCE AND PRESERVATION OF RECORDS

Snapmint 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. Snapmint will maintain for at least ten years from the date of cessation of transaction between the bank and the client, 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. Snapmint will also ensure 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 account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data will be made available to the competent authorities upon request.

III. MONITORING OF TRANSACTION

On-going monitoring is an essential element of effective KYC procedures. Snapmint can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. However, the extent of monitoring will depend on the risk sensitivity of the account. Since Snapmint will not have any deposit accounts, this situation will hardly arise, but Snapmint will in any case pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose or transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. Snapmint will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Snapmint will ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002 (and the Amended Act, 2009). It will also ensure that transactions of suspicious nature and/or any other type of transaction notified under section 12 of the PML Act, 2002 (and the Amended Act, 2009), is reported to the appropriate law enforcement authority.

CHAPTER IX – GENERAL

I. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

The Company shall envisage having an ongoing employee training programme so that the members of the staff are adequately trained in KYC 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 policies and implement them consistently and effectively.

a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the RE, regulation and related issues shall be ensured.

II. CUSTOMER AWARENESS

The Company shall take adequate measures to educate the customer on the objectives of the KYC programme, especially at the time of obtaining sensitive or personal information from the customers Wherever the Company desires to collect any information about the customer for the purpose other than KYC requirement, it shall not form part of the account opening form. Such information to be collected separately, purely on a voluntary basis in a form prescribed by the Company after explaining the objective to the customer and taking the customer's express approval for the specific uses to which such information could be put. The front desk staff must be specially trained to handle such situations while dealing with customers The Company shall also take care to see that implementation of the KYC guidelines in respect of customer acceptance, identification etc. do not result in denial of opening of new accounts and housing services to general public.

III. INTRODUCTION OF NEW TECHNOLOGIES - – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.

Snapmint shall pay adequate attention to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

IV. APPOINTMENT OF PRINCIPAL OFFICER

Snapmint has appointed a 'Principal Officer' who will be responsible for reporting all transactions and sharing of information. He will also be responsible to ensure that proper steps are taken to fix accountability for serious lapses and intentional contraventions of the KYC guidelines.

V. REPORTING TO FINANCIAL INTELLIGENCE UNIT OF INDIA

1) Snapmint shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

2) The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of at the time of reporting by Snapmint. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Snapmint which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those Companies, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

3) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Snapmint shall not put any restriction on operations in the accounts where an STR has been filed. Snapmint shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

4) Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

VI. REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS)

Reporting requirement under Foreign Account Tax Compliance Act (FATCA)and Common Reporting Standards (CRS) Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

- Register on the related e-filling portal of Income Tax Department as
- Reporting Financial Institutions at the link https:/ /incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution.
- Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61 Bor 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

  Explanation - Snapmint shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://wwwfedai.org.in/ RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules.

- Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.
- Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

- Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. REs may take note of the following:
    - updated Guidance Note on FATCA and CRS
    - a press release on 'Closure of Financial Accounts' under Rule 114H (8).
- In addition to the above, other United Nations Security Council Resolutions (UNSCRs) circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

CHAPTER - X

OTHER RESPECTIVE MEASURES:

I. SECRECY OBLIGATIONS AND SHARING OF INFORMATION:

a) Snapmint shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer.

b) 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.

c) While considering the requests for data/information from Government and other agencies, EHFL shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in transactions.

d) The exceptions to the said rule shall be as under:
   i. Where disclosure is under compulsion of law
   ii. Where there is a duty to the public to disclose,
   iii. the interest of bank requires disclosure and
   iv. Where the disclosure is made with the express or implied consent of the customer.

e) Snapmint shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

II. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

Snapmint shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

The 'live run' of the CKYCR has started with effect from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Snapmint shall take the following steps:

i. Snapmint shall upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

ii. Operational Guidelines (version 1.1) for uploading the KYC data have been released by CERSAI. Further, 'Test Environment' has also been made available by CERSAI for the use of REs.

III. SELLING THIRD PARTY PRODUCTS:

REs acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

i. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

ii. transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

iii. AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

iv. transactions involving rupees fifty thousand and above shall be undertaken only by:

   a. debit to customers' account or against cheques; and
   b. obtaining and verifying the PAN given by the account-based as well as walk-in customers.

v. Instruction at 'd' above shall also apply to sale of Snapmint's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.