SNAPMINT FINANCIAL SERVICES PRIVATE LIMITED

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

Version-4 July, 2024

Particulars	Details
Title	**KNOW YOUR CUSTOMER (KYC) & PREVENTION OF MONEY LAUNDERING (PMLA) POLICY**
Version	**4**
Review Date	**July 11, 2024**
Approved and Reviewed	**By Board**

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. 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.

OBJECTIVE:

The objective of KYC/AML policy is to prevent criminal elements for money laundering or terrorist financing activities. KYC procedures enable the company to understand its customers which in turn help them manage their risks prudently.

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).

1. **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.

2. **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.

3. **Compliance of KYC policy:**

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

- 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.

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.

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 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 company shall apply CDD measures at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.
e) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
f) Optional or additional information is obtained with the explicit consent of the customer after the account is opened.
g) CDD Procedure is followed for all the joint account holders, while opening a joint account.
h) If an existing KYC compliant customer of Snapmint desires to open another account, there shall be no need for a fresh CDD exercise.
i) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority
j) Circumstances in which a customer is permitted to act on behalf of another person/ entity, is clearly spelt out.
k) 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

l) The customer profile will include mandatory information for KYC purposes, such as customer's identity, address, social/financial status, nature of business activity and their location. The extent of Due Diligence will be determined by the perceived risk associated with the customer. The company will collect only the information relevant to the risk category and ensure it is not intrusive. This customer profile will be treated as a confidential document and its details will not be shared by any third party except where such sharing is as per statutory/regulatory requirement. The company shall ensure that the identity of the customer does not match with any person or entity whose name appears in the sanction lists circulated/prescribed by RBI from time to time.

*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. Where, Snapmint forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

RISK MANAGEMENT

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 the 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.

The risk categorisation of a customer and the specific reasons for such categorisation shall be

kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

(i) <u>High Risk–(Category A):</u>

High Risk Customers typically includes:

a) New to credit consumers;

b) Consumers with credit score below 700 and neither the primary mobile number or communication address (where positive confirmation is carried out by means of deliverables) is not stable in credit bureau or CKYC records or Aadhaar

(ii) <u>Medium Risk – (Category B):</u>

Medium risk Customers will include:

a) Credit bureau score is above 700 but none of Primary Mobile number and communication address (where positive confirmation is carried out by means of deliverables) is stable in credit bureau or CKYC records or Aadhaar

(iii) <u>Low Risk-(Category C):</u>

Customer carrying low risk may include the following:

a) Primary Mobile number or communication address (where positive confirmation is carried out by means of deliverables) is stable in credit bureau or CKYC records or Aadhaar
b) Salaried employees with well-defined salary structures;
c) Consumers with good credit score (700 and above) – salaried and self employed

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

Pursuant to the provisions of para 5A of the Master Direction - Know Your Customer (KYC) Direction, 2016, Snapmint is required to conduct a 'Money Laundering and Terrorist Financing (MLTF) Risk Assessment' periodically. This exercise aims to identify, assess, and effectively mitigate money laundering and terrorist financing risks associated with clients, countries or geographic areas, products, services, transactions, or delivery channels.

Furthermore, as per para 5B of the same regulations, Snapmint is mandated to apply a Risk-Based Approach (RBA) to mitigate and manage these identified risks, whether identified independently or through national risk assessment processes. This requires the Company to establish Board-approved policies, controls, and procedures tailored to effectively manage and mitigate these risks in accordance with regulatory requirements.

<u>a) Risk Based Approach for mitigation and management of risks</u>

As mandated, Snapmint shall apply a Risk Based approach for mitigation and management of the

risks. The company shall conduct a 'Money Laundering and Terrorist Financing Risk Assessment' exercise on annual basis. This exercise aims to identify, assess, and implement effective measures to mitigate money laundering and terrorist financing risks associated with clients, countries or geographic areas, products, services, transactions, or delivery channels.

During the assessment process, all relevant risk factors will be considered to determine the overall level of risk and the appropriate mitigation measures to be applied. Snapmint shall also incorporate sector-specific vulnerabilities that may be communicated by regulators or supervisors into its internal risk assessment.

b) ML/TF Risk Assessment Process

The risk assessment for a financial sector entity like an NBFC should be proportionate to its operations. Snapmint, being a smaller and less complex NBFC with simpler and limited loan products, may find a simplified risk assessment approach adequate. In contrast, larger NBFCs with complex loan products, multiple subsidiaries or branches offering diverse services, and a varied customer base, will necessitate a more sophisticated risk assessment process. This ensures that the level of scrutiny and risk management strategies are tailored to the specific complexities and scale of each NBFC's business operations.

Based on the guiding principles provided by the FATF and specific guidance issued by FATF for Banking and Financial sector, the process of risk assessment by NBFCs are as follows:

(i) Collection of information

Snapmint shall first collect information on various factors including information on general criminal environment, terrorist financing and information on specific factors pertaining to Terrorist Financing vulnerabilities, The information may be collected internally or externally

(ii) Threat indication

Based on information collected, NBFC shall identify jurisdiction and sector specific threats. The company shall take into account the level of inherent risk including the nature and complexity of their loan products and services, their size, business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location and countries of operation. The NBFC shall also look at the controls in place, including the quality of the risk management policy, the functioning of the internal oversight functions etc.

(iii) Assessment of ML/TF Vulnerabilities

The next step is to determine how the identified threats will impact the company. The information obtained shall be analysed in order to assess the probability of risk occurring. Based on the assessment, the MLTF risk should be classified as low, medium and high risk.

While assessing the risk, following factors should be considered:

- The nature, scale, diversity and complexity of the product/business
- Target Market
- The number of customers already identified as high risk
- The jurisdiction/ area of operations of the Company i.e. jurisdiction/area having higher level of corruption/fraud, organized crime and/or deficient MLTF controls as may be listed by RBI or FATF
- Internal Audit and Regulatory findings, if any
- The volume and size of the Transaction

Snapmint should complement the aforesaid information with information obtained from concerned internal and external sources such as official of the Company and list issued by regulator(s), and/or international/inter-governmental organizations and/or by the service provider.

The Risk Assessment shall be approved by the Senior Management of the Company. MLTF Risk Assessment Report shall be placed before the Board of Directors or Risk Management Committee of the Company on periodic basis as per the regulatory requirements.

(iv) Analysis of ML/TF Threats and vulnerabilities

After identifying and assessing MLTF threats and vulnerabilities, the next step is to consider how these factors interact to form an overall risk profile. This analysis should include an assessment of the likely consequences, allowing the Company to understand the potential impact and to devise appropriate risk mitigation strategies.

(v) Risk Mitigation

After analyzing threats and vulnerabilities, the NBFC must develop and implement policies and procedures to mitigate the identified ML/TF risks. Customer due diligence (CDD) processes shall be designed accordingly. While assessing credit risk, Snapmint shall also evaluate MLTF risk. Measures shall be implemented to prevent the misuse of legal persons or entities for money laundering or terrorist financing.

For medium or high-risk customers, or in the case of unusual transactions, the Company shall perform due diligence to identify the source and application of funds, the beneficiary of the transaction, and the purpose of the loan. Additionally, such customers shall be subject to ongoing due diligence as per the Company's KYC & AML Policy, in accordance with the Master Direction - Know Your Customer (KYC) Direction, 2016, as amended from time to time.

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 the relationship.

Snapmint's Customer Identification Program (CIP) shall be integrated in the AML policy in accordance with the PMLA Act 2002 and the relevant rules notified under the Act, which includes provisions requiring the business processes to:

a) Verify the identity of any person transacting with Snapmint to the extent reasonable and practicable

b) Maintain records of the information used to verify a customer's identity, including name, address and other identifying information

c) Consult sanction lists/FATF statements of known or suspected terrorists. Snapmint shall ensure that in terms of Section 51A of the Unlawful Activities Prevention Act (UAPA) 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC) and whose name appears in the sanction lists circulated by RBI

Snapmint shall ensure the compliance by verifying the name of the person or entity through the website of the concerned entity or via a service provider that offers third party verification services. This shall be in accordance with the applicable provisions and guidelines of the Rbi, the PMLA and the rules made thereunder.

Details of accounts or customers that bear resemblance to any individuals or entities on the list shall be treated as suspicious and be reported to FIU-IND, in addition to notifying the Ministry of Home Affairs as required under UAPA notification.

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 not be outsourcing any CDD activity to an outsourcing partner

CUSTOMER DUE DILIGENCE 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: PAN Number verified by the issuing authority

2. Proof of Possession of Aadhaar either with an equivalent e-document, OTP based e-KYC or CKYC identifier

3. Positive confirmation of communication address with a deliverable

4. First transaction is affected from customer's bank account

Or any other document prescribed as per the guidelines provided by RBI

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/license 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 Snapmint 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 Snapmint undertakes contact point verification and collects such other information and clarification as would be required to establish the existence of such a 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 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.

Snapmint shall perform verification of customer identity before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification, which may include verification through documents or non-documentary methods that are appropriate given the nature of the business process, the products and services provided, and the associated risks

PART IV- Accounts of Politically Exposed Persons (PEPs) residents outside India

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

Snapmint primarily offers its financial services to Indian customers only. If the Company extends any finance to non-residents, it should verify whether the individual is a Politically Exposed Person (PEP) and review all publicly available information about the person. The decision to transact with a PEP should be made only by the Head of Credit of the company supported by appropriate verification. Additionally, the Company must subject such accounts to enhanced ongoing monitoring. These norms also apply to the contracts of family members or close relatives of PEPs.

In case an existing customer or the beneficial owner of an existing account subsequently becomes a Politically Exposed Person (PEP), the approval of the Head of Credit shall be obtained to continue the business relationship. The account shall then be subjected to the KYC due diligence measures applicable to PEP customers, including enhanced ongoing monitoring

PART V- IDENTITY OF A BENEFICIAL OWNER

Snapmint shall identify the Beneficial Owners (BO) wherever required and take all reasonable steps to verify its identity. The term "beneficial owner" refers to the natural person who ultimately owns or controls a customer and/or the person on whose behalf the transaction is being conducted. This includes any individual who exercises ultimate effective control over a juridical person.

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

Explanation:

I. "Controlling ownership interest" means owning or being entitled to more than twenty-five percent of the shares, capital, or profits of the company.

II. II. "Control" includes the right to appoint the majority of the directors or to control the management or policy decisions, including through shareholding, management rights, shareholder agreements, or voting agreements.

(b) For a Partnership Firm: The beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical persons, has ownership of or is entitled to more than ten percent of the capital or profits of the partnership.

(c) For an Unincorporated Association or Body of Individuals: The beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical persons, has ownership of or is entitled to more than fifteen percent of the property, capital, or profits of such association or body of individuals.

(d) If No Natural Person is Identified under (a), (b), or (c): The beneficial owner is the relevant natural person who holds the position of senior managing official.

(e) For a Trust: The identification of beneficial owners shall include: The author of the trust, the trustee, the beneficiaries with a fifteen percent or more interest in the trust, Any other natural person exercising ultimate effective control over the trust through a chain of control or ownership. In cases where the customer is acting on behalf of another person as trustee or nominee, the

Company shall obtain satisfactory evidence of the identity of the persons on whose behalf they are acting.

(f) For Listed Companies or Their Subsidiaries: If the customer or the owner of the controlling interest is a company listed on a stock exchange or 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.

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, risk profile and risk based credit bureau checks;
2. 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 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.

ENHANCED DUE DILIGENCE

Snapmint is primarily engaged in retail finance and does not typically deal with customers who pose a high risk of money laundering, terrorist financing or political corruption. However, Snapmint shall conduct Enhanced Due Diligence (EDD) for all customers or accounts determined to pose a potential high risk and warrant enhanced scrutiny

Snapmint shall **a**dopt a risk-based approach to identify and investigate high-risk customers effectively, ensuring compliance with Anti-Money Laundering (AML) regulations. For high-risk customers, Snapmint shall obtain additional credentials to verify their identity and assess their risk level. Utilizing an advanced due diligence checklist, Snapmint shall gather all necessary details about the customer to ensure thorough evaluation and compliance. Additionally, Snapmint shall establish procedures to decline business or discontinue relationship with any customer when EDD cannot be adequately completed.

THIRD PARTY DUE DILIGENCE

For initial identity verification of customers Snapmint may rely on customer due diligence done by a third party, provided that records or information of such customer due diligence conducted by the third party are obtained within two days from either the third party itself or from the Central KYC Records:

(a) Snapmint shall take adequate steps 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.
(b) Snapmint is satisfied that the third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
(c) The third party is not based in a country or jurisdiction assessed as high risk.
(d) Snapmint is ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable.

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.

RING 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. <u>CUSTOMER AWARENESS</u>

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.

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, Snapmint 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.