Know Your Customer (KYC)/Anti-Money laundering (AML) / Combating of Financing Terrorism (CFT) Policy

Know Your Customer (KYC)/ Anti – Money Laundering (AML)/ Combating of Financing Terrorism (CFT) Policy

1. Background

The Government of India has enacted the Prevention of Money Laundering Act, 2002 (PMLA), to prevent money laundering and provide for the confiscation of property derived from or involved in money laundering. The Act came into force on July 1, 2005, and is amended periodically.

In consultation with the Reserve Bank of India (RBI), the Ministry of Finance, Department of Revenue, issued the Prevention of Money Laundering (Maintenance of Records) Rule, 2005 (PMLR), which has also been amended as necessary. Pursuant to the powers conferred by Section 35A of the Banking Regulation Act, 1949, read with Section 56 of the Act, and Rule 9(14) of PMLR, regulators issue directions on KYC standards for banks and financial institutions.

The Financial Intelligence Unit-India (FIU-IND), a body under the Government of India, is primarily responsible for coordinating and strengthening national and international efforts in intelligence, investigation, and enforcement against money laundering and related crimes.

Internationally, guidelines and recommendations pertaining to Know Your Customer (KYC) norms, Anti-Money Laundering (AML) measures, and Combating Financing of Terrorism (CFT) norms from the Financial Action Task Force (FATF), the Basel Committee on Banking Supervision, Wolfsberg Principles, etc., are followed.

This Group-wide Policy is designed to comply with the standards on KYC/AML/CFT obligations under the PMLA and relevant guidelines issued by regulators and law enforcement agencies. The Companies under the Group (Group) shall adhere to applicable guidelines and amendments related to KYC/AML/CFT under the PML Act 2002, the PMLR, and other pertinent laws.

2. Scope and objective of the Policy

i. Scope

This Policy sets the minimum unified standards for internal KYC/AML/CFT controls to mitigate legal, regulatory, reputational, operational, and financial risks. It applies to all outlets, offices, functions, and units of the Group, and should be read with relevant procedural manuals or operating guidelines.

The Group must follow the principles in this Policy. If any Company within the Group has unique KYC/AML regulations, stricter requirements of the two should be implemented in their KYC/AML/CFT procedures.

ii. Objectives

The guidelines aim to prevent the Group from being used for money laundering or terrorist financing. They help the Group understand its customers and their financial activities, managing risks like reputation more effectively.

The Policy establishes a strong framework for implementing KYC/AML/CFT standards throughout the Group. It ensures employee accountability for compliance with rules and regulations and supports law enforcement in combating money laundering and terrorist financing.

3. Definition of Money Laundering & Terrorism Financing

Money laundering is the process of making illegally gained money appear legal. It involves placing criminal proceeds into the financial system, layering them through transactions to obscure their origin, and integrating them back as legitimate funds.

Section 3 of PMLA, describes the offence of money laundering as follows:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering."

Terrorism financing is the collection or provision of funds intended to support terrorists or terrorist organizations, either to further their causes or carry out acts of terrorism.

4. AML Governance Structure & Risk Management Framework

1. Board & Senior Management

The Board of Directors or any Board Committee with delegated power shall approve the respective Company's (the Company) KYC/AML/CFT Policy. The Board and Senior Management must ensure the Policy aligns with regulatory provisions and international standards and update it regularly.

They are also responsible for implementing effective control processes to reduce the risk of money laundering or terrorist financing.

2. Designated Director

The Board will appoint a 'Designated Director' (DD) to ensure compliance with chapter IV of the PMLA. The CEO & Managing Director will serve as the DD. The Company will notify the Director of FIU-IND and the regulators of any changes to the DD's name, designation, address, and contact details, where required.

3. Principal Officer (PO)

As required under PMLA, the Company must appoint a Principal Officer (PO) at the management level. The PO will be appointed by the DD. The PO will act independently and, for administrative reasons, report directly to the Senior Management, the Chief Compliance Officer (CCO) for this purpose. The PO will not be nominated as the 'DD'. The name, designation, address, and contact details of the PO must be communicated to the FIU-IND and the regulators, where required, whenever there is a change.

The role and responsibilities of the PO include, but are not limited to:

- Overseeing and ensuring compliance with regulatory guidelines on KYC/AML/CFT issued periodically, and obligations under PMLA, rules, and regulations made thereunder.
- Reviewing the adequacy of KYC/AML/CFT systems and controls.
- Monitoring transactions, and timely submission of various reports and information to FIU-IND and regulators as per extant laws and regulations.
- Liaising with enforcement agencies and any other institutions involved in combating money laundering and financing of terrorism.

The PO and his/her team shall have timely access to KYC/AML/CFT related information within the Company. The PO will formulate procedures and manuals related to their function, which shall also detail roles and responsibilities.

5. AML Standards

The Group will use a Risk Based Approach (RBA) for its KYC/AML/CFT framework. The standards will focus on Customer Acceptance Policy, Risk Assessment, Customer Identification Procedures, and Transaction Monitoring.

i. Risk Based Approach (RBA)

The Risk-Based Approach (RBA) is crucial for effective KYC/AML/CFT standards implementation. It involves identifying, assessing, and understanding the risks the Company faces and taking measures to mitigate them.

The Company evaluates various factors to identify and assess ML/TF risk, including:

- Nature, scale, diversity, and complexity of business, products, and services
- Target markets
- Customer portfolio, especially high-risk customers
- Countries or jurisdictions connected to the Company's activities
- Distribution channels and reliance on third parties for CDD and technology use
- Internal audit and regulatory findings
- Methods of conducting identification and due diligence
- Transaction volume and size relative to company and customer profiles

Additionally, the Company follows RBI guidance notes on ML/TF Risk assessment and National Risk Assessment outcomes to determine RBA requirements as they are updated. The information required varies based on customer type (individual, corporate, etc.).

ii. Money Laundering and Terrorist Financing Risk Assessment by Company

a. The Company will regularly conduct ML/TF risk assessments to identify, evaluate, and mitigate money laundering and terrorist financing risks associated with customers, regions, products, services, transactions, and delivery channels.

b. All relevant risk factors will be considered to determine the overall risk level and necessary mitigation measures. The Company will also consider sector-specific vulnerabilities highlighted by regulators or supervisors.

c. Risk assessments will be documented according to the Company's nature, size, location, and complexity. Annually, the findings and action plans to address any gaps will be presented to the Board/Board Committee, which may adjust the assessment frequency based on the results.

d. Risk assessments will be conducted before launching new products, practices, services, or technologies.

iii. Know Your Customer (KYC) / Customer Due Diligence (CDD) Guidelines

The Company must collect customer information for all KYC/AML/CFT procedures to manage ML/TF risks effectively. KYC/CDD measures include verifying customer identity using reliable sources and understanding the purpose and nature of business relationships. These procedures are required at various stages:

- When starting an account-based relationship;
- If there are doubts about the customer's identification data;
- If there are suspicions of money laundering or terrorist financing;
- When selling third-party products as agents for more than INR 50,000;
- During transactions with walk-in customers involving amounts equal to or exceeding INR 50,000, whether single or connected transactions;
- If a customer appears to be structuring transactions below the INR 50,000 threshold intentionally.

iv. Customer Acceptance Policy

The Customer Acceptance Policy (CAP) establishes the general criteria for accepting customers and constitutes an essential aspect of the Policy.

a. The Company will not engage with shell companies or institutions, nor with any entity that permits its accounts to be used by shell companies.
b. Caution is exercised when dealing with foreign companies located in jurisdictions with inadequate AML/CFT measures.
c. The Company shall avoid opening or maintaining any anonymous accounts or conducting transactions with such accounts. A Suspicious Transaction Report (STR) may be filed if necessary, where the customer is fictitious, operating under a benami name, acting on behalf of undisclosed persons, or when the Company cannot verify the identity of the customer or obtain required documentation due to non-cooperation or unreliable information provided by the customer.
d. When opening accounts through professional intermediaries, the Company will ensure that:
    - Customers are identified when their accounts are opened by a professional intermediary on behalf of an individual customer.
    - Accounts are not opened through intermediaries bound by confidentiality obligations that prevent disclosure of customer details to the Company.
e. When establishing relationships with Politically Exposed Persons (PEPs), the Company shall:
    - Implement systems to identify whether a customer is a PEP.
    - Obtain senior management approval before opening or continuing an account for a PEP.
    - Collect sufficient information about the sources of funds/wealth in accounts of family members and close associates of PEPs and verify publicly available information where necessary.

- Conduct Enhanced Due Diligence (EDD) and enhanced ongoing monitoring, supported by appropriate risk management procedures.

Adherence to the CAP should not impose undue restrictions on customers or result in denial of services, especially to economically and socially disadvantaged individuals. However, in cases of regulatory restrictions, the Company will not provide services to those individuals or entities.

v. Customer Identification & Due Diligence

i. Customer Identification

Customer identification involves due diligence when starting an account-based relationship, including verifying the customer and beneficial owner with reliable sources. The Company collects documents and information based on the customer's risk level, adhering to PMLA and regulatory guidelines. The due diligence level depends on the perceived risks.

Mandatory & Officially Valid Documents (OVD)

a. The Company will strictly comply with the guidelines issued by Regulators/PML rules on obtaining mandatory information such as PAN or Form 60, a certified copy of any OVD containing details of identity and address, one recent photograph for identification purposes, and other relevant information/documents pertaining to the nature of business and financial status of the customer, as specified by the Company.

b. The PAN shall be verified through the issuing authority's verification facility. Additionally, the Company will adhere to the regulatory guidelines regarding the acceptability of PAN or Form 60, OVDs, or deemed OVDs as permissible, and follow any restrictions advised by regulators where prescribed CDD measures are not completed, with appropriate notification to customers.

c. In accordance with regulatory guidelines, the Company shall validate Aadhaar using authentication or offline verification services provided by UIDAI, as applicable, and follow procedures with explicit customer consent as outlined in regulatory or Aadhaar Act guidelines. The modes of authentication or offline verification through permissible channels and relevant conditions/requirements will be followed as per regulatory guidelines when required.

d. Where a customer submits proof of possession of an Aadhaar number, containing the Aadhaar number, the Company will ensure the customer redacts or blacks out their Aadhaar number appropriately when Aadhaar number authentication is not required under Section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act (Aadhaar Act).

e. If a customer undertakes Aadhaar authentication using the e-KYC facility of the Unique Identification Authority of India (UIDAI) and wishes to provide a current address different from the address available in the Central Identities Data Repository (CIDR), the Company will collect a self-declaration to that effect.

f. The use of Aadhaar and proof of possession of Aadhaar will be in accordance with the Aadhaar Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019, and the regulations made thereunder.

g. The Company will also follow guidelines regarding the acceptability of OVDs with marriage certificates or gazette notifications where the name has changed post-issuance.

h. When obtaining OVDs, the Company will ensure that copies are verified against the original documents and certified accordingly. All employees/authorized officials of the Company are authorized to carry out such verification and certification. In the case of Non-Resident Indians (NRIs) or Persons of Indian Origin (PIOs), alternatives to the OVD copy being certified by a Company official include certification by:
   - Authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
   - Branches of overseas banks with which Indian banks have relationships,
   - Notaries Public abroad,
   - Court magistrates,
   - Judges,
   - Indian Embassies/Consulates General in the country where the non-resident customer resides.

i. The customer may submit a KYC Identifier to the Company for retrieval of KYC records from the Central KYC Records Registry (CKYCRR) as specified by the regulators. The Company will ensure that explicit consent from the customer is obtained for downloading records from CKYCRR using the KYC identifier and will also validate the KYC documents. The Company will retrieve the KYC records online from the CKYCRR using the KYC Identifier, and the customer will not need to submit the same KYC records or additional identification documents unless:

   - There is a change in the customer's information in the CKYCRR records;
   - The Company deems it necessary to verify the customer's identity or address, perform enhanced due diligence, or develop an appropriate risk profile;
   - The validity period of documents downloaded from CKYCR has expired; or
   - The KYC record retrieved is incomplete or does not comply with current KYC norms.

j. When relying on third parties for customer identity verification, the Company will:

   - Obtain customer due diligence records or information immediately from the third party or CKYCRR;
   - Ensure that copies of KYC documents and relevant information are available from the third party without delay;
   - Verify that the third party is regulated, supervised or monitored and complies with CDD and record-keeping requirements;
   - Avoid third-party reliance from high-risk jurisdictions.

   For legal persons or entities, the Company will:
   - Verify the legal status through constitutional documents;
   - Obtain proper authority documentation for authorized persons;
   - Understand the source of funds, ownership, control structure, and identify natural persons controlling the legal entity.

k. Customer identification will be undertaken via:

- **Physical KYC**: Physical verification of KYC documents by authorized officials.

- **Digital KYC**: Capturing live photos and valid documents along with location details.

- **Video-based Customer Identification (V-CIP)**: Secure audio-visual interaction for customer identification and due diligence.

- **Non-face-to-face KYC**: Methods like Aadhaar OTP-based e-KYC, CKYCR, Digilocker, and Aadhaar Offline XML.

ii. Customer Due Diligence

a) The Company will follow CDD procedures for customers when sanctioning loans and managing authorized signatories, beneficial owners or power of attorney holders related to legal entities. The Company is responsible for CDD and EDD measures where applicable and will ensure that decision-making functions for KYC compliance are not outsourced.

b) New relationships and existing customers will be assigned a Unique Customer Identification Code (UCIC).

c) An existing KYC-compliant customer seeking another loan or service with unchanged KYC details may rely on existing records without fresh KYC & CDD procedures. Similarly, customers with completed KYC verification, who wish to transfer their account/relationship between branches, may do so without fresh KYC procedures if not due for periodic updating.

d) The Company will establish due diligence procedures for various types of entities such as sole proprietorships, companies, partnerships, trusts, societies, and others. When opening accounts for non-natural persons, reasonable measures will be taken to identify and verify beneficial owners in line with regulatory guidelines, with exceptions allowed under specific guidelines.

e) If a customer acts on behalf of another entity, the Company will clearly define circumstances according to established law and practice, ensuring verification of mandate holders' identities along with customers' identities as per guidelines.

f) Suspicion of money laundering or terrorism financing, or doubts about previously obtained customer identification data, will prompt the Company to review due diligence measures, including re-verifying customer identity and obtaining business relationship information. If CDD processes raise suspicion, the Company will file an STR with the regulator instead of continuing CDD.

g) For non-face-to-face customers, higher-risk mitigation procedures will accompany usual CDD processes.

h) Customers will be informed that updated documents must be submitted within 30 days to comply with regulatory requirements.

i) Additional or exceptional measures, like obtaining recent photographs or physical presence, can be mandated where necessary but will not impose restrictions or adverse actions during periodic updates. However, the Company may restrict accounts of non-cooperative customers.

j) Mandatory KYC information required for opening an account or periodic update will be specified by the Company, while optional details will only be requested post-account opening with explicit customer

consent. The Company will keep customer information confidential and not use it for cross-selling purposes without permission.

k) The Company will capture and share KYC information as per stipulated templates during onboarding or upon receiving updated information. This will be shared with CKYCRR according to regulatory guidelines and operating rules. Upon KYC updates by any Regulated Entities (REs), CKYCRR will inform all REs dealing with the concerned customer, and the Company will retrieve and update the KYC record accordingly.

l) For non-face-to-face mode mobile number changes, two-level verifications will be carried out, and notifications will be sent to both old and new contact details. Detailed operational processes will be reviewed and approved by relevant forums.

vi. Customer Risk Categorisation (CRC)

The customer profile should include information about the customer's identity, legal entity type, social/financial status, nature of business activity, and location. When verifying a customer's identity, the ability to confirm identity documents online or other services offered by issuing authorities should be considered. Additionally, it should contain details such as nationality, annual income, turnover, product and customer type, etc. The information collected from different customer categories should be non-intrusive. Based on this profile information (gathered directly or indirectly), customers will be categorized into three risk parameters: High, Medium, or Low Risk. The level of due diligence will depend on the perceived risk.

For risk categorization, individuals and entities whose identities and sources of wealth can be easily identified and whose transactions generally match their known profile may be categorized as 'Low Risk'. Customers who pose higher-than-average risks to the Company should be categorized as medium or high risk based on their background, nature and location of activities, country of origin, source of funds, and customer profile. The Company will apply Enhanced Due Diligence (EDD) measures for higher-risk customers when necessary.

In cases of unusual or suspicious transactions/applications or when a customer's risk profile changes to high risk, appropriate EDD measures will be implemented as outlined in the KYC/AML/CFT procedures. Customer profiles must be updated periodically based on the assigned risk level, and activities must be monitored according to a predetermined profile, with special attention given to higher-risk customers or activities.

The customer profile is confidential and will not be used for cross-selling or similar purposes. The Company will only seek relevant and non-intrusive information from customers based on their risk category. The confidentiality of customer risk ratings will be maintained, and staff will ensure that risk ratings and the reasons for them are not disclosed to customers at any time.

The Company will conduct ad hoc or trigger-based reviews and periodic reviews of risk categorization based on transaction patterns and significant changes in profile data to assess the need for applying EDD measures. Event-based ad hoc or trigger reviews and periodic risk categorization reviews will be conducted at least once every six months.

Based on these guidelines, the Company will develop appropriate risk-based due diligence, technology (systems), and transaction monitoring procedures to implement a Risk-Based Approach (RBA).

7. Economic and Trade related sanctions and combating the Financing of Terrorism

Sanctions are an important tool used by governments and international/national bodies, such as UNSCR, MHA, RBI, OFAC, and FATF, to enforce their decisions through various acts, including UAPA and WMD. Sanctions can range from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or diplomatic restrictions. Sanctions regimes are dynamic in nature and subject to frequent changes. The Group will ensure compliance with applicable sanctions regimes and will have a procedure in place for this purpose.

The Group will implement a mechanism for enhanced monitoring of accounts suspected of having terrorist links, enabling swift identification of transactions and prompt reporting to FIU-IND. The Company will update its negative database using lists of individuals and entities provided by the aforementioned national and international government bodies. The Group will ensure that it does not maintain any accounts for individuals or entities appearing on these lists. Any account with similarities will be reported to regulators or government agencies according to the relevant procedures under UAPA.

The Group will strictly follow the procedures outlined in the UAPA and comply with orders (freezing, unfreezing, etc.) issued by regulators and government agencies as per existing laws and procedures.

The Group will adhere to regulatory norms, including effective enhanced due diligence measures proportionate to the risks, business relationships, and transactions. It will also rely on publicly available information related to jurisdictions that do not or insufficiently apply FATF recommendations to assess its relationships and transactions with customers and countries falling under this category, recording such assessments and preserving them for future use by regulators or government agencies.

The Group will conduct screening of customers (individuals or legal entities), service providers/vendors, board members, employees, etc., during onboarding and ongoing stages against the 'Negative Database' to ensure that these relationships do not pose additional risks to the Company. The Group will verify that the identities of these individuals do not match those of persons or entities listed in sanction lists circulated by various regulators.

For this purpose, the Company will maintain a system/application to update the negative database and check it against its customers to identify any matches. In case of a match, upon verification, the Company will treat them as suspicious and report them to designated authorities in compliance with existing regulations.

8. Ongoing monitoring of transactions & reporting

The Company will monitor customer transactions according to predefined rules, which the PO will periodically frame and review. High-risk accounts will undergo more thorough monitoring.

Additionally, beyond the Red Flag Indicators (RFIs) recommended by FIU-IND, the Company may create suitable RFIs or alert scenarios tailored to its business model.

The Company will close system-generated alerts promptly, following detailed guidelines in the transaction monitoring procedures. In accordance with PML Rules, information will be reported in electronic or manual format within FIU-IND timelines, covering:

- Cash transactions based on specified parameters
- Transactions involving counterfeit currency
- Suspicious transactions
- Non-profit Organizations Transaction Reports
- Any other reports requested by regulators, government, enforcement agencies, or FIU-IND

The Company will exercise ongoing due diligence regarding business relationships, risk profiles, and sources of funds/wealth with all customers, closely examining transactions to ensure they align with available knowledge of the customers, their businesses, and risk profiles. Where necessary, the source of funds will also be examined.

No restrictions will be placed on account operations where an STR has been filed, ensuring no tipping off to the customer at any level within the Company. However, confidentiality may not apply when sharing information among companies for analyzing unusual transactions and activities.

To enhance KYC/AML/CFT awareness among staff and generate alerts for suspicious transactions, the Company may consider best practices and guidance from prominent organizations. Suitable procedures and systems will be developed to facilitate the filing of unusual transaction reports and other requisite reports by field functionaries.

9. Updation/ Periodic Updation

Updation/Periodic Updation refers to the steps taken to ensure that documents, data, or information collected under the CDD process are kept current and relevant, especially in high-risk cases, by periodically reviewing existing records. The Company will conduct periodic updates for each customer based on their assigned money laundering risk. This periodicity will be at least every 2, 8, and 10 years for High, Medium, and Low risk customers, respectively, from the date of account opening or the last KYC update. The facility for submitting documents for periodic updates will be available at all Company branches, regardless of the branch where the customer holds an account. The Company may carry out the updation/periodic updation exercise through any of the following methods:

In case of Individual

- **No change in KYC information:** A Self-declaration shall be obtained from the customer or obtain KYC records online from CKYCR, based on customer's consent, by using KYC identifier

- **Change in KYC information:** The Company will obtain a self-declaration from the customer detailing the new address. The Company will then verify the address through positive confirmation within two months, using methods such as an address verification letter, contact point verification, or receipt of deliverables.

  The Company may also use other methods like Aadhaar OTP Based e-KYC in non-face-to-face mode for updating periodic KYC records of individual customers.

In case other than individuals

- **No change in KYC information:** A self-declaration in this regard shall be obtained from the customer or obtain KYC records online from CKYCR, based on customer's consent, by using KYC identifier

Change in KYC information: In the event of a change in KYC information, the RE will undertake the KYC process equivalent to that applicable for onboarding a new LE customer.

10. Account Closure

If the Company cannot apply KYC measures due to lack of information or non-cooperation from the customer, or if the customer refuses to submit PAN/Form No.60, it may terminate the relationship after due notice or restrict account operations to credits only.

VI. Introduction of New Technologies

The Company will address ML/TF threats from new technologies and apply current KYC procedures before introducing new products or services. Due diligence and KYC measures will also be applied to agents marketing loans when applicable.

VII. Internal Controls & Audit Mechanism

i. Employees

All units should promptly report any suspicious activity or transaction to the PO or their team upon reasonable suspicion.

ii. Internal Auditors

The internal audit scope includes testing compliance with KYC/AML/CFT policies. Auditors will check and verify policy application at units and branches and report any lapses. Ensure the audit team is properly staffed with trained personnel familiar with KYC/AML/CFT policies and regulations.

iii. Audit Committee of the Board

Compliance and audit findings will be periodically presented to the Board's Audit Committee for review.

VIII. Data management & Record Preservation

The following steps shall be taken regarding maintenance, preservation, and reporting of customer account information, in accordance with the provisions of the PML Act and Rules and the Company's approved Policies on Preservation of Documents and Archival of Records. The Company shall:

- Maintain all necessary records of transactions (both domestic and international) between the Company and the customer for at least 5 years from the date of the transaction.
- Preserve records pertaining to the identification of customers and their addresses obtained while establishing the relationship and during the business relationship for at least 5 years after the relationship has ended. These identification records shall include data, account files, business correspondence, and results of any analysis undertaken.
- Maintain a record of the NPO registration on the DARPAN portal for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.
- Make available the identification records and transaction data swiftly to competent authorities upon request.

- Introduce a system for maintaining proper records of transactions as prescribed under PMLR.
- Maintain all necessary information in respect of transactions prescribed under PMLR to permit reconstruction of individual transactions, including the following details:
  - The nature of the transactions;
  - The amount of the transaction and the currency in which it was denominated; • The date on which the transaction was conducted; and
  - The parties to the transaction.
- Develop a system for the proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly when required or requested by competent authorities.
- Maintain records of the identity and address of customers, as well as records of transactions referred to in Rule 3, in hard or soft format.
- All records shall be maintained in line with the Policy for Preservation and Archival of Documents of the Company.
- Maintain records in respect of transactions carried out with walk-in customers.

IX. Sharing of Information Amongst Group Companies

The Group is dedicated to responsibly sharing data among group entities. All customer due diligence and identity verification activities will strictly follow applicable regulations. Data related to ML/TF risk management will be exchanged among the PO of group companies with the highest confidentiality and privacy.

X. Co-operation with the Regulators & Secrecy

The Group shall co-operate with regulators and designated law enforcement and investigative agencies in accordance with applicable laws and regulations. The Company shall also undertake countermeasures when required by any international or intergovernmental organization of which India is a member and accepted by the central government.

Secrecy Obligations and Sharing of Information

The Company is committed to maintaining the confidentiality of customer information that arises from the contractual relationship between the Company and the customer.

Information collected from customers for the purpose of account opening shall be treated as confidential and shall not be disclosed for cross-selling or any other purposes without the explicit permission of the customer.

When considering requests for data or information from the Government and other agencies, the Company shall ensure that the requested information is not of a nature that would violate the provisions of laws related to secrecy in banking transactions.

Exceptions to this confidentiality rule are permitted in the following circumstances:

- When disclosure is compelled by law,
- Where there is a duty to the public to disclose,
- When the interests of the Company require disclosure,

Where disclosure is made with the express or implied consent of the customer.

XI. Employee Hiring and Accountability

The Group will integrate an effective screening mechanism into its hiring process, including verifying identities and checking names against negative or criminal lists. Each employee plays a crucial role in implementing a strong KYC/AML/CFT program by efficiently performing their duties. Any suspicious behavior will be addressed appropriately.

The Group aims to ensure that staff involved in KYC/AML/CFT matters possess integrity, ethical standards, understanding of current standards, communication skills, and adaptability to changes.

Employees must maintain confidentiality of customer information, reports made to FIU-IND/regulators, and avoid 'tipping off' customers.

XII. Employee Training & Awareness

The Group will maintain an ongoing employee training program on KYC/AML/CFT standards, ensuring staff are well-trained in these policies. Training methods will be coordinated with HR's Learning & Development Department and tailored for frontline staff, compliance staff, and those handling products, services, and customers. Service providers and Board members will receive training as needed.

XIII. Customer Education

The Group will inform customers about the objectives of the Bank's KYC/AML/CFT program by preparing specific literature or pamphlets and hosting relevant information on the Company's website. The Company will use various customer touchpoints, including branches and the website, to achieve the goal of customer education.

XIV. FATCA/CRS/Income Tax

Under FATCA and CRS, the Company will follow Income Tax Rules 114F, 114G, and 114H and maintain procedures for reporting requirements.

XV. Exception Handling

If laws outside India prevent implementing KYC guidelines, the company must inform the RBI.

XVI. Policy Validity and Review

The Board of the Companies under the Group shall review this Policy once every three years, subject to any regulatory or statutory amendments necessitating an earlier review.

Annexure – Glossary

Account

Account is defined generally, as any formal business relationship established to effect financial transactions and shall have the same meaning as defined by RBI and SEBI in various product types. An account is any formal business relationship for financial transactions, as defined by RBI and SEBI across different product types.

AML (Anti-Money Laundering)

Anti-money laundering (AML) is a term used for the regime/program followed by financial and legal institutions, which includes set of laws, regulations and practices designed to prevent, detect, and report money laundering activities. Anti-money laundering (AML) refers to laws, regulations, and practices used by financial and legal institutions to prevent, detect, and report money laundering.

Aadhaar Number

“Aadhaar number", means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and includes any alternative virtual identity generated under sub-section (4) of that section.

Aadhaar Authentication

” Authentication”, in context of Aadhaar Authentication means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, based on information available with it.

Authorized Official

To verify the original of the Officially Valid Document (OVD) and record it on the copy, the Company may authorize its employees as well as Direct Selling Agents (DSA) and their staff. These authorized personnel will sign a declaration stating that they have seen and verified the original document (OSV) on the copy of the OVD, including their employee code and the unique code assigned to the DSA.

Beneficial Owner

The beneficial owner is the individual who has a controlling ownership interest or exercises ultimate control over a legal entity. For detailed definitions, refer to the RBI Master Direction, 2016 as amended.

Central KYC Records Registry (CKYCRR)

“Central KYC Records Registry” (CKYCRR) 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.

Chief Compliance Officer

The Head of Compliance Department in SMICC who is entrusted with the responsibility of overseeing the management of Compliance Risk across the Company and at the Group Entities (as applicable), as per laid down framework. The Head of the Compliance Department at SMICC is responsible for overseeing the management of compliance risk throughout the Company and its Group Entities, in accordance with the established framework.

Common Reporting Standard (CRS)

CRS means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Transaction Matters.

Company

Company (SMFG India Credit Company Ltd) or Group Company (SMFG India Home Finance Company Ltd) will have the same meaning in the context of this Policy.

Customer

'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 (e.g. Beneficial owner) who is engaged in the transaction or activity, is acting. The 'transactions' shall have the same meaning as defined in the PMLA Rules and Act.

Deemed OVDs

The following documents are termed as deemed OVDs for limited purpose of proof of address:

a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
b) Property or Municipal tax receipt; pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
c) 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
d) Listed companies and leave and license agreements with such employers allotting official accommodation

Note: The customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'a-d' above.
In case 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

Designated Director

” Designated Director" means a person designated by the reporting entity (Company, financial institution, etc.) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes: -

(i) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company

Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) refers to additional checks beyond standard due diligence, applied when there's a high risk of money laundering or terrorist financing. EDD can involve intensive transaction monitoring, frequent KYC updates, customer verification, and other measures like penny drop and customer calls.

FATCA

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 U.S. taxpayers, or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

FATF

The Financial Action Task Force (FATF) is an inter-governmental body established by the Ministers of its Member jurisdictions, to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

Group

"Group" refers to SMFG India Credit Company Ltd and SMFG India Home Finance Company Ltd, as defined in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961.

Intermediary

As per the provisions of the PMLA, intermediary includes a stockbroker, sub-broker, share transfer agent banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depositary participant, merchant banker, underwriter, portfolio manager, investment advisor and any other intermediary associated with the securities market and registered under Sec 12 of the SEBI Act, 1992.

KYC (Know Your Customer)

KYC is an acronym for “Know your Customer”, a term used for customer identification process. It involves making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, the nature of customer’s business, reasonableness of operations in the account in relation to the customer’s business, etc. which in turn helps the companies to manage their risks prudently.

KYC Templates

Templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

Negative Database

Negative Database means the list of banned entities/individuals considered as associated with activities like terrorism etc., and countries against which sanctions have been imposed by organizations like UN, OFAC, and/or circulated by RBI, MHA, FIU-IND etc.

Non-face-to-face customers

Customers who open accounts without visiting the branch/offices of the Company or meeting the authorized officials of the Company.

Non-profit organisations (NPO)

Any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013

Offline Verification

"Offline Verification" 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

Officially Valid Document (OVD)

OVD means the passport, proof of possession of Aadhaar Number, the driving license, 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, letter issued by the National Population Register containing details of name, address.

Note: 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.

Person

In terms of PML Act a 'person' includes: An individual, a Hindu undivided family, a company, a firm, an association of persons, or a body of individuals, whether incorporated or not, every artificial juridical person, not falling within any one of the above persons, and any agency, office or branch owned or controlled by any of the above persons.

Politically Exposed Person (PEP)

Individuals (whether as customer or beneficial owner) who are or have been entrusted with prominent public functions by a foreign country including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials

Principal Officer

Principal Officer (PO) means an officer nominated by the Company, responsible for furnishing information as per rule 8 of the PML Rules.

Proceeds of Crime

Proceeds of crime refer to any property derived from or obtained, directly or indirectly, through the commission of offence scheduled under PMLA.

Records

The term 'Records' shall include the records maintained in the form of books or stored in a disk, floppy/micro film etc. and any other electronic storage device or such other form as may be prescribed.

Regulators

Regulators include but are not limited to, Reserve Bank of India (RBI), Securities Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI) & Financial Intelligence Unit - India (FIU-IND),

Regulated Entities

Regulated Entities means all categories of Banks defined in Banking Regulation Act, All India Financial Institutions (AIFIs), All categories of NBFCs defined in Scale Based Regulations, Asset Reconstruction Companies (ARCs), All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers), All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

Senior Management

The term "Senior Management" for the purpose of this Policy includes concerned direct reports of the CEO & MD, either singly or jointly.

Shell Company

A shell company is one that lacks a physical presence in its country of incorporation and isn't part of a regulated financial group under consolidated supervision. Physical presence requires significant management within the country. A local agent or minimal staff doesn't qualify as physical presence.

Suspicious Transaction

Suspicions transaction means a transaction referred to in clause (h) of the PMLA rules, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no economic rationale or bonafide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

Tipping Off

'Tipping off' means informing/communicating to the customer (directly or indirectly) that his account has been or would be reported to regulators for suspicious activity pertaining to money laundering or terrorist financing.

Transaction

"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and include

a) Opening of an account;
b) Deposits, 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;
c) The use of a safety deposit box or any other form of safe deposit;
d) Entering into any fiduciary relationship;
e) Any payment made or received in whole or in part of any contractual or other legal obligation; or
f) Establishing or creating a legal person or legal arrangement.

Unique Customer Identification Code (UCIC)

The Unique Customer Identification Code (UCIC) will help Company to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable financial institutions to have a better approach to risk profiling of customers.

Walk-in Customer

A person who does not have an account-based relationship with the bank but undertakes transaction with the company.

Abbreviations

UAPA – Unlawful Activities (Prevention) Act

RBI – Reserve Bank of India
UN – United Nations
OFAC – Office of Foreign Assets Control
WMD – Weapons of Mass Destruction
FATF – Financial Action Task Force
MHA – Ministry of Home Affairs