Know Your Customer (KYC) Guidelines & Anti-Money Laundering Standards (AML) Policy

DECIMUS FINANCIAL LIMITED

MAY-2022

AS APPROVED BY THE BOARD OF THE COMPANY.

Contents

Glossary

RBI	Reserve Bank of India
CAP	Customer Acceptance Policy
CIP	Customer Identification Procedures
PMLA	Prevention of Money Laundering Act
PEP	Politically Exposed Person
KYC	Know Your Customer
AML	Anti-Money Laundering
NY	DECIMUS FINANCIAL LIMITED
NBFC	Non-Banking Financial Companies
CTR	Cash Transaction Report
STR	Suspicious Transaction Report
FIU –IND	Financial Intelligence Unit – India
CIBIL	Credit Information Bureau (India) Limited
UIDAI	Unique Identification Authority of India
OVD	Officially Valid Document
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest
CDD	Customer Due Diligence
NRI	Non-Resident Indian
PIO	Person of Indian Origin
V-CIP	Video based Customer Identification Process
LE	Legal Entity

1. Preamble

The Reserve Bank of India (RBI) had advised all the NBFCs to ensure that a proper policy framework on Know Your Customer and Anti Money Laundering measures is formulated and put in place with approval of the Board. The policy was to lay down the systems and procedures to help control financial frauds, identify money laundering and suspicious transactions, combating financing of terrorism and careful scrutiny/ monitoring of large value of cash transactions. Pursuant to advice from the RBI, a Know Your Customer and Anti Money Laundering Policy (the Policy) was put in place with approval of the Board on June 23, 2006.

Since then, the Policy has been reviewed and revised with the approval of the Board, in line with the notifications on AML KYC issued RBI from time to time.

Presently, the Policy is proposed to be revised with the approval of the Board, to comply with the modification effected by RBI to its KYC Master Directions on May 10, 2021.

2. Definitions

Customer

'Customer' is defined to mean a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person, on whose behalf the person who is engaged in the transaction or activity, is acting.

Transactions

The regulatory norms define transaction as:

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

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) Entering into any fiduciary relationship.
d) Any payment made or received in whole or in part of any contractual or other legal obligation;
e) Establishing or creating a legal person or legal arrangement.

Officially Valid Documents (OVD)

"Officially Valid Document" (OVD) means the passport, the driving license, proof of

possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that, where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. The customers should be asked to redact or blackout Aadhaar number and the functions responsible should ensure that same.

Beneficial Owner

A beneficial owner is a natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

Certified Copy

Certified copy means comparing the copy of officially valid document with the original and recording it on the copy by the authorized officer of FICC in a manner prescribed by RBI. In the case of Non-Resident Indian (NRI)/Person of Indian Origin (PIO) customers, the following officials also could certify the copy of the OVD

a. Authorized officials of overseas branches of Scheduled Commercial Banks registered in India
b. Branches of overseas banks with whom Indian banks have relationships
c. Notary Public abroad
d. Court Magistrate
e. Judge
f. Indian Embassy/Consulate General in the country where the non-resident customer resides.

For purpose of verifying the original of the OVD and recording it on the copy, FICC might authorize the Direct Selling Agents (DSA), Fintech Partners and their employees. Such authorized officers will sign the declaration of having seen and verified the original (OSV) on the copy of the OVD with their employee code along with the unique code allocated to the DSA/Fintech partner

Non-face to face Customer

Non-face-to-face customer means customer who opens accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

Digital KYC

Capturing live photo of the customer or OVD or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the Company OR

uploaded by customer. Uploading of KYC image of PAN, AADHAR or Govt. issued proof.

Equivalent e-document

An electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per Rule 9 of the Information Technology (Preservation and

Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016. This may be obtained for individuals and also from non-individual customers.

Video based Customer Identification Process (V-CIP)

A method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for Customer Due Diligence (CDD) purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Policy.

3. Policy Objectives

The basic objectives of the policy:

a. To comply with the guidelines issued in Prevention of Money Laundering Act (PMLA), 2002.
b. To adhere the "Know Your Customer" (KYC) policies and procedures issued by Reserve Bank ofIndia.
c. To prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

4. Scope

KYC and AML Policy guidelines are applicable to all the functions of the organization dealing with customers, vendors / service providers and employees. Functions should adhere to the guidelines mentioned in this policy while drafting their internal policies, procedures, products etc.

This policy should be read in conjunction with related operational guidelines issued from time to time by Compliance/Risk.

Know Your Customer policy envisages the following key elements:

a. Customer Acceptance Policy (CAP)
b. Customer Identification Procedures (CIP)

c. Monitoring of transactions
d. Risk management

5. <u>Customer Acceptance Policy (CAP)</u>

For the Customer Acceptance following criteria should be followed:

a. No account should be opened in anonymous or fictitious/benami name(s) and accept customers only after verifying their identity, as laid down in Customer Identification Procedures (discussed later).
b. Parameters of risk perception should be defined in terms of customer identity, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status. Customer should be categorized as low, medium and high risk. The organization should seek only such information from the customer, which is relevant to the risk category and is not intrusive.
c. Documentation requirements and other information should be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act 2002 and guidelines issued by Reserve Bank from time to time.
d. Not to open an account where the organization is unable to apply appropriate customer due diligence measures. i.e., the organization is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished.
e. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediaryin the fiduciary capacity.
f. Necessary checks should be conducted in CIBIL / Credit Information Company, any notified list of RBI or any other Regulator before accepting the customer and opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations.
g. The existing customers and new employees during hiring would be screened against the consolidated list of individuals and banned entities circulated by RBI to ensure that there are no matches.
h. All the customers would be screened through Sanctions list of Office of Foreign Assets Control (OFAC) of US Department of Treasury at the time of on-boarding.
i. Customer profile should be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes within the Company without the express permission of the customer.
j. For sharing the customer information obtained from UIDAI, for sharing the same with other entities, specific permission from UIDAI should be obtained.

The above Customer Acceptance Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

6. Risk Categorization

For the purpose of risk categorization, individuals (other than High Net Worth), entities whose identities & source of wealth can easily be identified and entities with accounts having transactions by & large confirming with known profile should be categorized as Low Risk. The examples of low-risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc.

Customers who are likely to pose a higher-than-average risk to the organization should be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client's profile etc. The organization should apply enhanced due diligence measures based on the risk assessment thereby requiring intensive due diligence for higher risk customers especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence may include (a) non- resident customers (b) high net worth individuals
(c) trusts, societies, charitable organizations etc. (d) companies having close family shareholding or beneficial ownership. (e) Firms with 'sleeping partners', (f) non-face to face customers and (h) those with dubious reputation as per public information available, etc.

Full KYC exercise will be required to be done at least every two years for high risk, eight years for medium risk and ten years for low-risk individuals and entities taking in to account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained. Physical presence of such clients is not insisted upon at time of periodic updating. Furthermore, in case of low-risk customers, the organization should not seek fresh proofs of identity and address at time of periodic updating, in case of no change in status with respect to their identities and addresses. A self-certification by a low-risk customer to this effect would be taken as sufficient. In case of change of current address of such low-risk customers, the organization should seek a certified copy of the document (proof of address) by mail/post etc.

7. Periodic updating of KYC

a. Individual Customers:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard to be obtained through customer's email-ID, customer's mobile number registered with us, Mobile application, Letter etc.

ii. **Change in address:** A copy of OVD or deemed OVD or equivalent e-documents as per KYC Policy for the new address to be obtained from the customer through customer's email-ID, customer's mobile number registered with us, Mobile application app and Letter etc.

b. Customers other than individuals:

i. No change in KYC information: in case of any change in the KYC information of the LE customer, a self- declaration to be obtained from the LE customer through its email ID registered, mobile application, letter from an official authorized by the LE in this regard, board resolution etc. Beneficial Ownership (BO) information available to be reviewed and updated.

ii. Change in KYC information: To undertakes the KYC process equivalent to that applicable for on-boarding a new LE customer.

c. Additional measures:

i. If the validity of the CDD documents available with us has expired at the time of periodic updating of KYC, KYC process equivalent to that applicable for on-boarding a new customer to be undertaken.

ii. Customer's PAN details, if available, to be verified from the database of the issuing authority at the time of periodic updating of KYC.

iii. An acknowledgment is to be provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updating.

iv. The information / documents obtained from the customers at the time of periodic updating of KYC are to be promptly updated in our records / database and an intimation, mentioning the date of updating of KYC details,is to be provided to the customer.

iv. Facility of periodic updating of KYC to be made available at any branch,

During periodic updating, customers' KYC details are to be migrated to current Customer Due Diligence (CDD)standards as per updated KYC Policy

If an existing KYC compliant customer desires to open another account with the organization, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

8. <u>Customer Identification Procedure (CIP)</u>

The organization should identify the customer and verifying his/ her identity by using reliable independent sources of documents, data or information to ensure that the customer is not a fictitious person.

The organization should be able to satisfy the competent authorities that due diligence was observed based on risk profile of the customer in compliance with extant guidelines in place. Besides risk perception, the nature of information / documents required would also depend on the type of customer (individual, corporate etc.)

Identification as under, would be required to be obtained in respect of different classes of customers:

a. Customers that are natural persons:
   i. Address/location details/camera
   ii. Identity Proof and Recent photograph
b. Customers that are legal persons:

i. Legal status of the legal person/entity through proper and relevant documents.
ii. Verification that any person purporting to act on behalf of the legal person/entity is soauthorized and identity of that person is established and verified.
iii. Understand the ownership and control structure of the customer and determine who are the enatural persons and ultimately control the legal person.

Individual Customers (Mandatory Pan Number)

a. The customers would submit OVD or upload details for identity and address.
b. Individual customers have to mandatorily submit the Permanent Account Number or Form No. 60. This would also apply to individuals who are beneficial owner, authorized signatory or power of attorney holder related to any legal entity.

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

Proprietorship Firms

Documents which could be obtained as proof of business/activity for proprietary firms (any one), in addition to the documents of the proprietor as individual:

a. Registration Certificate
b. Certificate/ license issued by the Municipal authorities under Shop & Establishment Act,
c. Sales and Income tax returns,
d. CST / VAT/GST certificate (Provisional/Final)
e. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of Director General of Foreign Trade (DGFT)/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statue
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 the name of the proprietary concern

Any one of the above documents in the name of the proprietary concern would suffice Partnership Firms:

Where the customer is a partnership firm, the certified copies of the following

documents should beobtained:

a. PAN of the partnership firm
b. Certificate of registration
c. Partnership deed.
d. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf
e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalfalong with any OVD for identity and address proof and one recent photograph of such persons.

Trusts

Where the customer is a trust firm, the certified copies of the following documents should be obtained:

a. PAN/Form No. 60 of the entity
b. Certificate of registration
c. Trust deed.
d. Power of Attorney granted to a member or an employee of the firm to transact business on its behalf
e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalfand any OVD for identity and address proof and one recent photograph of such persons.

Unincorporated Bodies

Where the customer is an unincorporated association or a body of individuals, the certified copies of thefollowing documents should be obtained:

a. PAN/Form No. 60 of the entity
b. resolution of the managing body of such association or body of individuals;
c. power of attorney granted to him to transact on its behalf
d. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalfand any OVD for identity and address proof and one recent photograph of such persons.

Companies:

Where the customer is a Company, the certified copies of the following documents should be obtained:

a. PAN of the Company
b. Certificate of incorporation
c. Memorandum and Articles of Association
d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with their Permanent Account Number or Form 60 and anyOVD or Aadhaar card for identity and address proof and one recent photograph of such persons.

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

i. Document showing name of the person authorized to act on behalf of the entity;
ii. Officially valid document for proof of identity and address in respect of the person holding an attorney to transact on its behalf and one recent photograph and
iii. Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

9. <u>Beneficial Ownership</u>

The organization should determine the beneficial ownership and controlling interest in case of applicants who are not individuals and the KYC of the beneficial owners should be completed. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice.

S. No.	Applicable for	Guide lines	
(i)	Where the client isa company	The beneficial owner is the natural person(s), who, whether acting aloneor together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means	a. Ownership of/entitlement to more than 25 % of shares or capital or profits of the company b. Control shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
(ii)	Where the client isa partnership firm or a company	The beneficial owner is the natural person(s), who, whether acting aloneor together, or through one or more juridical person	Ownership of/entitlement to more than 15% of the capital or profits of the partnership
(iii)	Where the client is an unincorporated association or body of individuals	The beneficial owner is the natural person(s), who, whether acting aloneor together, or through one or more juridical person	Ownership of/entitlement to more than 15% of the property or capital or profits of such association or body of individuals

(iv)	Where no natural person is identified under (i), (ii) or (iii) above	The beneficial owner is the relevant natural person who holds the positionof senior managing official
(v)	Where the client is a trust	The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% percent or more

		interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership
(vi)	Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company	Not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies

There are certain indicative guidelines issued by RBI from time to time for customer identification requirements with regard to matters, such as Trust / Nominee or Fiduciary Accounts, Accounts of companies & firms, Client Accounts opened by professional intermediaries, Accounts of Politically Exposed Persons resident outside India and Accounts of non-face-to-face customers and these guidelines should be adhered to the extent applicable.

1. <u>Unique Customer Identification Code (UCIC) :</u>

Every customer should be provided with a unique customer identification code. This will help to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the organization to have a better approach to risk profiling of customers.

2. <u>Customer Due Diligence (CDD)</u>

For undertaking CDD, either of the following should be obtained from an individual or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

S No	Nature of the Document	Type of Verification
I	Proof of possession of Aadhaar number where offline verification can be carried out	Offline/online verification
II	Proof of possession of Aadhaar number where offline verification cannot be carried out	Digital KYC as specified under Annex - I

III	Any OVD or uploading by customer containing the details of identity and address	Digital KYC as specified under Annex – I
IV	Any equivalent e-document of any OVD containingthe details of identity and address	Verification of Digital signature and Live photo as specified under Annex - I

Note: For a period not beyond such date as may be notified by the Government for the NBFCs, instead of carrying out Digital KYC, certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph (where an equivalent e-document is not submitted) may be obtained.

a. Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962

b. The live V-CIP may be carried out by an official of the Company, for establishment of an account based relationship with an individual customer, after obtaining informed consent with adherence to stipulations as per Annex - II

c. Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. Offline Verification means the process of verifying the identity of the Aadhaar number holder without authentication, through suc h offline modes as may be specified by the Aadhaar regulations.

In case the CDD is outsourced, then the records or the information of the customer due diligence carried out by the third party should be obtained within two days from the third party or from the Central KYC Records Registry. In such cases, decision-making functions of determining compliance with KYC norms should not be outsourced.

CDD procedure should be applied at the UCIC level and if an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

In case of Video based Customer Identification Process (V-CIP):

V-CIP may be carried out for

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. In case of CDD of a proprietorship firm, equivalent e-document of the activity proofs with respect to the proprietorship firm should be obtained, as mentioned in Sec. 7.2 of this Policy apart from undertaking CDD of the proprietor.

ii) Updating/Periodic updating of KYC for eligible customers

10. Record Retention

Records pertaining to identification of the customer and his address obtained while opening his account and during course of business relationship should be preserved for at least five years after the business relationship has ended.

All necessary records of transactions of the customer, both domestic and international, should be maintained for at least five years from the date of transaction.

1. Accounts of Politically Exposed Persons (PEPs) resident 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. Decision to deal with such persons as a customer shall be taken up at a senior management level (SVP and above) and should be subjected to enhanced monitoring. The norms are also applied to the accounts of the family members or close relatives of PEPs.

In case of an existing customer or beneficial owner of an existing account subsequently becoming PEP, matter should be reported to senior management level and be subjected to enhanced monitoring.

2. Accounts of non-face-to-face customers:

In the case of non-face-to-face customers, it should be ensured that the first payment is effected through the customer's KYC-complied account with another regulated entity or customer shall upload all KYC documents online.

3. Central KYC Registry (CKYCR)

The customer KYC information should be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities (LE)' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

The customer information related to LEs should be submitted to CKYCR for accounts of LEs opened onor after Apr 1, 2021.

For accounts of LEs opened prior to Apr 1, 2021 and account of Individuals opened prior to Jan 01, 2017, KYC records are to be uploaded to CKYCR during the periodic updating, (carried out once in every two years for high risk customers, eight years for medium risk and ten years for low risk) or earlier as and when KYC information is obtained/received from customer.

Further, during periodic updating, customers' KYC details are to be migrated to current Customer Due Diligence (CDD) standards.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records could be retrieved online from CKYCR and customer is not required to submit any KYC records unless

a. there is a change in information of customer as existing in the records of CKYCR;
b. current address of customer is required to be verified;
c. it is considered necessary to verify identity or address of customer, or to perform enhanced duediligence or to build an appropriate risk profile of the client.

KYC Identifier generated by CKYCR, should be communicated to the Individual/LE.

11. Monitoring of Transactions

The organizations monitoring activity should depend on the risk sensitivity of the account and high value cash transactions. High risk accounts should be subjected to intensified monitoring.

All transactions including those of suspicious nature like "a customer who is reluctant to provide information needed for a mandatory report, an account where there are several cash transactions below a specified threshold level to avoid filing of reports, employee whose lavish lifestyle cannot be supported by his or her salary, negligence of employee / willful blindness is reported repeatedly " etc. should be reported to the Compliance Head on a monthly basis.

Cash Transaction Report (CTR) in respect of cash transactions of INR 1 Million and above undertaken in an account either single or in an integrally connected manner in a calendar month should be reported to FIU – IND by 15th of the succeeding month.

Suspicious Transaction Report (STRs) should be reported to FIU – IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash or a series of transactions integrally connected are of suspicious nature. A customer whose transaction is reported as Suspicious to FIU should be treated as "high risk" customer for a period of one year from the date of reporting. For STR reporting, the "Suspicious Transaction Monitoring and Reporting Policy" as approved by Board during its meeting held on Sep 8, 2016 would apply.

The organization should put in place a system of periodic review (at least once in six months) of risk categorization of accounts and need for applying enhanced due diligence measures.

The organization should maintain proper records of series of cash transactions of a customer below INR 1 Million but monthly aggregate exceeding INR 1 Million and the records related to transactions reported as suspicious transactions to FIU – India. These records should be retained for a period of five years from the date of transaction.

The Company should adhere to the provisions of Income Tax Rules 114F, 114G and 114H and submit reports as per the process laid down under Foreign Account Tax Compliance Act (FATCA)and Common Reporting Standards (CRS)

12. Risk Management

Concurrent/Internal Audit

Concurrent / Internal Auditors should have a process to verify the compliance with KYC/AML policies and procedures across the organization including the application of KYC procedures at the branches and comment on the lapses observed. The compliance in this regard should be put before the Audit Committee of the Board on quarterly basis.

Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise should be carried out annually to identify, assess and take effective measures to mitigate the money laundering and terrorist financing risk arising from clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The risk assessment should be commensurate to size, geographical presence, complexity of activities/structure, etc. of the Company. The risk assessment should also take cognizance of the overall sector-specific vulnerabilities, if any, that RBI may share time to time.

Risk Based Approach (RBA) should be applied for mitigation and management of risks identified and Board approved policies, controls and procedures in vogue should be accordingly aligned.

Proper staffing of the audit function with persons adequately trained and well -versed in AML/CFT policies of the Company, regulation and related issues will be ensured.

Hiring of Employees and Employee training

All the prospective employees will be screened through the UNSCR Terrorist list as part of due diligence process. All the existing employees will be screened through the new additions to the UNSCR Terrorist list every month

There should be ongoing employee training program so that the staff is adequately trained in KYC Policy and procedures. As the employees' roles could undergo change, all the employees (including frontline staff, compliance staff and staff dealing with new customers), will undergo training covering all aspects of KYC Policy including empowering them to handle issues arising from lack of customer education.

13. Customer Education

The organization should prepare specific literature / pamphlets etc., to educate the customer of the objectives of the KYC program. The frontline lending and operating managers

should be fully equipped with the compliance requirements of KYC guidelines in respect of new customer acquisition and shall adhere to the Customer Identification & Acceptance procedure.

14. KYC for the Existing Accounts

KYC norms are applicable to all the existing customers in a time bound manner. Where the organization is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the debit operations should be stopped.

15. Principal Officer and Designated Director

The senior management officer (SVP and above) should be the Principal Officer for KYC/AML matters who will be responsible for implementation of and compliance with this policy. His duties, in this regard, will be as follows:

a. Overall monitoring of the implementation of the organization's KYC/AML policy.
b. Monitoring and reporting of transactions, and sharing of information, as required under the law.
c. Timely submission of Cash Transaction Reports (CTRs), Suspicious Transaction Reports (STRs) to FIU-IND.
d. Maintaining liaison with the law enforcement agencies, banks and other institutions, which are involved in the fight against money laundering and combating financing of terrorism.
e. Ensuring submission of periodical reports to the Top Management /Board.

The Managing Director or a whole – time Director should be appointed as the "DesignatedDirector" for ensuring compliance with the obligations under the PMLA, 2002.

16. Review of the Policy

This Policy should be reviewed if there are any amendments in the regulatory guidelines and the revised policy should be staged for Board's Approval in the subsequent Board Meeting post the amendments are notified by the regulator.

Annex - I Digital KYC Process

A. A Digital KYC Application (KYC App) mobile app of loan for digital KYC process is to be made available at customer touch points and is to be undertaken only through this authenticated application of the Company

B. Access of the KYC App to be controlled and be ensured that it is not used by any unauthorized person.
C. KYC App to be accessed only through Login-ID and Password, Live OTP or Time OTP controlled mechanism given to the authorized officials of the Company
D. Customer, for KYC, should visit the location of the authorized official of the Company or vice- versa. The original OVD should be in possession of the customer.
E. Live photograph of the customer should be taken by the authorized officer and the same photograph should be embedded in Customer Application Form (CAF).
F. KYC App should add a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the customer.
G. KYC App should have a feature such that only live photograph of the customer is captured and not printed or video-graphed photograph.
H. Background behind the customer should be white and no other person should come into frame
I. Live photograph of original OVD or proof of possession of Aadhaar (if offline verification is not being done) placed horizontally, should be captured vertically from above and water-marking as stated above should be done. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.
J. Live photograph of customer and original documents should be captured in proper light so that they are clearly readable and identifiable.
K. All the entries in the CAF should be made as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details.
L. Once the above- m e n t i o n e d process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' is to be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF.
M. In case, the customer does not have his/her own mobile number, mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.
N. In any case, the mobile number of authorized officers registered with the Company should not be used for customer signature.
O. It must be verified that mobile number used in customer signature is not mobile number of authorized officers.
P. Authorized officer should provide a declaration about capturing live photograph of customer and original document. For this purpose, authorized official should be verified with OTP sent to the mobile number registered with the Company. This OTP validation is to be treated as authorized.

   officer's signature on the declaration. Live photograph of authorized official should also be captured in the authorized officer's declaration.
Q. Subsequent to all these activities, the KYC App should give information about the completion of the process and submission of activation request to an activation officer of the Company, and also generate transaction-ID/reference-ID number of the process.

Authorized officer should intimate the details regarding transaction-ID/reference-ID number to customer for future reference.

R. Authorized officer of the Company should verify that
   i. information available in picture of document is matching with information entered in CAF
   ii. live photograph of the customer matches with the photo available in the document
   iii. all the necessary details in CAF including mandatory fields are filled properly

S. On Successful verification, the CAF should be digitally signed by authorized officer of the Company and a print of CAF, should be bear signatures/thumb-impression of customer at appropriate place

T. The signed document should be scanned and uploaded in system and the original hard copy should be returned to the customer.

U. The customer should register on Mobile app with opt.

V. Customer should upload KYC documents and photographs for Identification and address verification.

Annex – II Video Customer Identification Process (V-CIP)

A. Live V-CIP should be carried out by an official of the Company after obtaining customer'sinformed consent

B. Video of the customer should be recorded along with photograph

C. For identification of the customer, offline verification of Aadhaar should be conducted

D. Clear image of PAN card displayed by customer should be captured, except in cases where e- PAN is provided. PAN details should be verified from Income Tax department.

E. Live location of customer (Geotagging) should be captured to ensure that customer is physically present in India

F. Photograph in Aadhaar/PAN details should match with the customer and the identification details in Aadhaar/PAN should match with details provided by customer.

G. Sequence and/or type of questions during video interactions should be varied in order to establish that interactions are real-time and not pre-recorded.

H. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the XML file or QR code generation date should not be older than 3 days from the date of carrying outV-CIP.

I. Accounts opened through V-CIP should be operational only after being subjected to concurrent audit

J. Process should be seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt.

K. Liveliness check should be carried out in order to guard against spoofing and such

other fraudulent manipulations.

L. To ensure security, robustness and end to end encryption, software and security audit and validation of the V-CIP application should be carried out before rolling it out.

M. Interaction should be triggered from the domain of the Company, and not from third party service provider

N. Process should be operated by officials specifically trained for this purpose and activity log along with the credentials of the official performing the V-CIP should be preserved.

O. Video recording should be stored in a safe and secure manner and bear the date and time stamp

(a) <u>Assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies may be taken, to ensure the integrity of the process as well as the information furnished by the customer.</u> V-CIP Infrastructure

(i) Comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

(ii) Ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the RE. Appropriate artificial intelligence (AI) technology can be used to ensure thatthe V-CIP is robust.

(vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber-security event under extant regulatory guidelines.

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live

environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure:

(i) Organization shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Organization specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

(iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

(iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

(v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

(vi) The authorized official of the Organization performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a) KYC records downloaded from CKYCR, in accordance with Master direction, using the KYC identifier providedby the customer

b) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi Locker

Organization shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of Master Direction.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Organization shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. Further; Organization shall ensure that no incremental risk is added due to this.

(vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

(ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(c) V-CIP Records and Data Management:

(i) The entire data and recordings of V-CIP shall be stored in a system / system located in India. Organization shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this RBI Master Direction, shall also be applicable for V-CIP.

(ii) The activity log along with the credentials of the Organization official performing the V-CIP shall be preserved.

Sanjeev Srivastava
Director