KYC/AML/CFT Policy

Introduction

Our Company, Capital Finserve Limited has been licensed and authorised by the Reserve Bank of India (RBI) for the NBFC Services

As notified by the RBI, the PML (Amendment) Act, 2009 brings all Reporting Entities (including financial institutions like UFSL) within the ambit of PMLA, 2002.

Further directions from the RBI also mandates, among others, the appointment of a Principal Officer, the appointment of a Designated Director, having a Policy Framework for AML/CFT/KYC and its periodic updation, Implementation of a Customer Acceptance Policy/Customer Identification Procedure & Risk Profiling, Reporting of Cash Transactions and Suspicious Transactions to the FIU-IND.

All the Reporting Entities are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions in terms of the provisions of PMLA 2002, the PML (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India.

The purpose of our AML policy is to establish the general framework for the fight against money laundering, terrorism, corruption, proliferation financing and other financial crimes. We understand that the successful participation in this fight by the financial sector requires an unprecedented degree of global cooperation between governments and financial institutions. Our organisation is committed to review our AML strategies and objectives on an ongoing basis and to maintain an effective AML program. We require management and employees to adhere to these standards in preventing the use of our products and services for money laundering purposes.

Adherence to this policy is fundamental for ensuring that our entire network, regardless of geographic location, complies with applicable anti-money laundering legislation. It is the responsibility of all employees to keep ill-gotten funds out of our institution.

The Company, since then, had been preparing, implementing, and updating Policy Framework for AML/CFT/KYC. considered the suggested amendments and prepared the revised policy to include the guidelines issued by the RBI till date. Any regulatory changes after this program shall be adopted and incorporated by the Company on the time periods as required by the regulators. Each stakeholder is expected to ensure strict/complete adherence to this policy while undertaking their corresponding activities.

The policy framework on AML/CFT/KYC of the company is as under:

2. Objectives, Scope, and Application of the Policy

The primary objective of the Policy is to prevent our branch/ franchisee /agency network from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

This policy aims:

(i) To prevent criminal elements from using our branches and associates for money laundering activities

(ii) To enable the branches and associates to know and understand the customers and their financial dealings better which in turn, would help to manage risks prudently

(iii) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

(iv) To comply with applicable laws and regulatory guidelines.

(v) To ensure that the concerned staff are adequately trained in AML/CFT/KYC procedures.

This Policy is applicable to all branches/offices / network of business associates of the company and must be read in conjunction with related operational guidelines issued from time to time.

3. Definition of Customer

To KYC policy, a 'Customer' is defined as:
o A person who undertakes occasional/regular transactions (*A person with whom the RE has got a transaction-based relation OR an account-based relation*)
o an entity that has a business relationship with us
o One on whose behalf the transaction is made (i.e. Ultimate Beneficiary)

4. Money Laundering

4.i. Definition of Money Laundering as per Sec.3 of PMLA, 2002

Section 3 of the Prevention of Money Laundering Act, 2002 defines offence of money laundering as under:

"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."

4.ii. Different stages involved in Money Laundering are.

(a) Placement, (b) Layering; and (c) Integration.

a. Placement:

The first stage is successfully disposing of the physical cash received from illegal activity. Money laundering is a "cash-intensive" business, generating vast amounts of cash from illegal activities. The monies are placed into the financial system or retail economy or are smuggled out of the country. The aim of the Launderer is to remove the cash from the location of acquisition so as to avoid detection by the authorities and then to transform it into other asset forms.

b. Layering:

While layering, there is an attempt at concealment or to disguise the source of ownership of the funds by creating complex layers of financial transactions, also designed to disguise the audit trail and provide anonymity. The purpose of layering is to disassociate the illegal monies from the source of the crime by intentionally creating a complex web of financial transactions aimed at concealing any audit trail as well as the source and ownership of funds. Round-tripping, a combination of transactions involving transfer of money across jurisdictions, eventually resulting in a return to the jurisdiction of origin, mainly to avoid taxes, is also used a mode of layering.

c. Integration:

The final link in money laundering process is called the integration stage. It is this stage at which the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the Launderer making it appear to have been legally earned. By this stage, it is extremely difficult to distinguish legal and illegal wealth.

4.iii. Definitions of Proliferation Financing & Weapons of Mass Destruction and their Delivery Systems

Financing of Proliferation or Proliferation Financing ('PF') refers to the act of raising/providing funds, other assets, or financial services, to persons or entities for purposes of WMD proliferation, including the Proliferation of their means of delivery or related materials.

WMD (Weapons for Mass Destruction) Proliferation refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both Dual-Use technologies and goods used for non-legitimate purposes).

4.iv. Stages of Proliferation Financing

(a) Raise
(b) Disguise
(c) Procure and Transport

Often proliferation financing involves companies in or near a sanctioned country and accounts under the control of a foreign national (i.e. not Iranian or a North Korean national) with sympathies to the sanctioned country. This, combined with the use of false documentation, allows proliferators to avoid detection.

5. Guidelines

5.1 General

The Company shall ensure that information sought for from the customers is not intrusive but relevant to the perceived risk and strictly in conformity with the RBI guidelines. Irrelevant information shall be avoided. Additional information, if any, shall be obtained from the customer, wherever necessary, but with the customers' consent. The information obtained shall not be divulged for cross selling or any other purpose and the confidentiality of the information collected shall be always maintained.

5.2 KYC Process

As per the Rule (9) of PMLA, it is the responsibility of the entity to identify its clients, verify their identity, obtain information on the purpose, and intended nature of business relationship and determine whether client is acting on behalf of a beneficial owner, and if so, take all steps to verify the identity of the beneficial owner.

KYC is the process of due diligence to be undertaken by financial institutions/ intermediaries to identify and locate an entity or individual to ensure that the financial transactions are not part of money laundering, terrorist financing or proliferation financing. The process involves –

(a) Identification of the customer in-person using minimum one of the Officially Valid Documents (OVDs) prescribed by the Regulator from time to time; and

(b) Address proof of the customer where he generally resides and is available in case of need, using minimum one of the Officially Valid Documents (OVDs) prescribed by the Regulator from time to time.

(c) PAN & Recent Photograph – In case, the individual is establishing an account-based relationship, or the individual happens to be the owner / partner / promoter / trustee/director/PoA holder/Authorised Signatory of any legal entity establishing a relation with us. The Permanent Account Number (PAN) as obtained shall be verified from the verification facility of the issuing authority.

(d) Wherever equivalent e-document of any OVD is collected from the customer, the digital signature shall be verified as per the provisions of the Information Technology Act, 2000 (21 of 2000).

KYC procedure also enables us to know/understand our customers and their financial dealings better which in turn, help us to manage our risks prudently.

The KYC program of the Company has been framed incorporating the following 4 key elements, as mandated by the RBI:

(a) Customer Acceptance Policy.
(b) Customer Identification & Verification Procedure.
(c) Monitoring of Transactions; and
(d) Risk Management.

5.2.1 Customer Acceptance Policy (CAP)

Customer Acceptance Policy has been framed in such a way that it is non-discriminative but adheres to the spirit of the guidelines prescribed under the PMLA/RBI guidelines. Our policy shall always be customer friendly, and we shall not look at each and every customer with suspicion but shall be on alert to detect any miscreants trying to establish a relation with us.

Acceptance of any person as a customer and the KYC compliances to be adhered to, shall be subject to and governed by the board approved policy.

Enhanced due diligence shall also be conducted when dealing with Politically Exposed Persons, the detailed procedure for which has been set out, under a separate paragraph below.

The Company's Customer Acceptance Policy shall always be based on the following as directed by RBI:

(a) The Company shall not conduct transactions in anonymous or fictitious/benami names or through any third party and all transactions shall be put through only against:

    i. Personal application (as applicable); and
    ii. Proof of Identity/Address/PAN/Photograph as explained in the KYC Process under clause 5.2 of this document.

(b) The Company shall not accept any customer/undertake any transaction where it is unable to verify the identity and/or obtain documents to ascertain the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to it.

(c) Whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, we shall carry out full scale customer due diligence before accepting the customer/ undertaking any transactions.

(d) Whenever a customer is required to be substituted by another person for un-avoidable reasons, we shall check and verify that the person is clearly authorised by the customer (detailing the Relation/ID/Address/Signature of the substitute) to transact on his behalf. KYC process also shall be applied on both.

(e) Customer Due Diligence shall be applied at UCIC (Unique Customer Identification Code) level and therefore shall not be repeated for opening another account or availing a different service, except when any additional information is to be collected as per any regulatory guideline.

5.2.1. a. Officially Valid Document (OVD)

The documents accepted by the Company as Proof of Identity and/or Address shall include any document as prescribed by RBI from time to time, through its master directions on KYC.

These are known as Officially Valid Documents (OVD). Any change made in the list of OVDs accepted by the Company shall be subject to RBI guidelines. Any single OVD may be sufficient to prove the identity and address. Certified copy shall mean comparing the copy with its original and recording the same on the copy by way of a seal and sign by the authorised employee at the PoS.

Names different from what appears on the OVD shall be acceptable only if the OVD is provided along with Government Gazette notification indicating Name Change or Marriage Certificate issued by the concerned State Government.

5.2.1. b. Customer Profile

As per the instructions of RBI, a profile of each customer with whom a business relationship is established, must be prepared. Most of our customers being walk-in clients, we have transaction-based relations rather than account-based relations as done in banks. Accordingly, it may not be possible to prepare a detailed profile of customers who undertake only a single transaction with us. However, a brief customer profile containing information relating to customer's identity, address, contact details, etc., shall be maintained. At the same time, a comprehensive due diligence process shall be applied on any customer who wishes to establish an account-based relationship with us. The company may make use of online or other services offered by the issuing authorities for confirming the reliability of identity documents of the customers, wherever possible. The nature and extent of due diligence, among other things, depend upon the risk perceived by us and the customers shall also be categorized accordingly. Updating the profiles of customers shall be an ongoing and continuous process and shall be conducted depending upon the risk categorization of the customer as well as changes, if any, in the data reported by the customer. All details provided and included in the customer profile shall be confidential and shall not be divulged by the Company for cross selling or any other purposes.

5.2.1. c. Sanctions Screening

The Company shall not conduct transactions in cases where, the identity of the customer matches with any person with known criminal background or shell companies/banks or unlicensed banks/shadow banks/remittance agents/exchange houses/money transfer agents or entities supporting them, or with banned entities such as individual terrorists or terrorist organisations etc. whose name appear in the FATF and OFAC or other sanction lists published by RBI or any other regulators, along with our internal watch lists including adverse media from time to time. Automated screening solutions shall be made use of to achieve complete insulation from those blacklisted. The Company shall also not allow stripping, whereby important information related to sanctions, payments or instructions is either altered or intentionally removed.

5.2.1. d. Periodic Updation & Termination of relationships

As per regulatory guidelines, the periodic updation of KYC is to be done at least once in ten, eight and two years for customers, respectively.

However, we have incorporated this process along with the risk review so that both become more efficient and meaningful. CDD measures need to be applied at the time of periodic updation for Individuals and Non-Individuals in cases where there are changes to the existing details and fresh certified copies or its equivalents are to be obtained as proofs. It shall be ensured that CDD is conducted in compliance with Part V, Sec 38 of the Master Direction. System alerts are to be provided for KYC updation & the related logs shall be maintained in the system in an easily retrievable manner.

Business relationships shall be subject to closure if initiated by the customer him/herself or by the Company in case of any default or involvement in any financial crime. Inclusion in the sanction's lists shall also be considered appropriately for account closures.

5.2.2 Customer Identification & Verification Procedure

Each transaction shall be through only after personal identification of each customer. While verifying the customer's identity, any online verification facility available or other services offered by the issuing authorities shall also be made use of. The customers must come to our counter for putting through the transactions and in exceptional cases, the authorised official of the company may provide the service at the doorstep of the customer i.e. either at his/her office or residence.

Video based customer identification process (V-CIP) shall be adopted as an alternate method of customer identification process with facial recognition and customer due diligence by the authorised official of the company by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. The company shall ensure that this process shall adhere to all prescribed standards and procedures as prescribed by the regulator from time to time.
Non-face-to-face onboarding shall be adopted as another alternate method of customer identification process where the customer is not met physically or through V-CIP. Here, the company shall make use of digital channels such as CKYCR & Digilocker for onboarding the customer in a non-face-to-face mode. The risk profile of the customers onboarded via non-face-to-face mode shall always be categorised as high & shall be subject to EDD until IPV or V-CIP is done. PAN shall mandatorily be obtained from such customers and shall be verified with the issuing authority. To prevent fraud, transactions shall be permitted only from this mobile number. System shall not allow to link an alternative mobile number with this the customer profile, post CDD, for transaction OTP/updates.
The company shall take reasonable steps to collect and confirm the email ID and mobile number of the customer. The mobile number shall be verified with the service provider. In case of a name difference, the mobile number shall only be accepted, if the customer is able to provide documentary evidence to establish a relationship with the actual owner of the mobile number and a consent in case of non-family members.

Any change in mobile number after CDD as above shall be done only after completing the whole process again.

5.2.2. a. Individuals

The customer shall be required to fill in a prescribed form, sign the same in the presence of the authorized officials of our Company and the application should be accompanied by duly signed photocopies of any one of the OVDs. This process can be substituted partially or completely with any alternative methods prescribed by the Regulator. This Besides, if the address in OVD differs from the current address, the customer shall produce original Telephone Bill, Bank account statement, ration card, letter from employer etc. which is not more than two months old. The customer shall submit OVD with current address within a period of three months. The original documents shall be returned after verification and branch official need to be certify the OVD. The Company shall not insist on separate address proof, where the photo ID document submitted by the customer also bears the current permanent address.

The customer identification procedure shall also involve due diligence of the customer by way of enquiring about his activities, nature of business/profession, status in the society, frequency of travel, sources of funds etc. All details of the customer shall be fed into our system besides preserving hard copies of the documents. In case of foreign tourists, copies of passport containing identification particulars and address shall be accepted for both identification and address. Further a copy of the VISA of non-residents, duly stamped by immigration authorities shall also be obtained by the Company and kept on record. Customers availing third party services/products through us need not undergo the procedures as detailed above until the value of the services/products availed surpasses the threshold set by the regulators from time to time.

5.2.2. b. non-individuals

In the case of legal persons i.e. entities such as Companies/Firms etc. the customer Identification Programme shall involve obtaining copies of documents or information in support of their existence such as:

i. Sole Proprietary Firms

Information:

(i) Business Name
(ii) Address
(iii) Telephone/Fax Number/email

Certified copy each of the following documents

(i) Registration certificate / GST certificate / Shops & Est Registration
(ii) Any officially valid document identifying the proprietor
(iii) Address Proof – Electricity bill/Water bill/Land line Telephone bill
(iv) Photograph & PAN Card of the Proprietor

ii. Partnership Firms Information:

(i) Legal name
(ii) Address
(iii) Names of all partners and their addresses
(iv) Telephone/Fax numbers of the firm and partners

One certified copy each of the following:

(i) Registration certificate / GST certificate / Shops & Est Registration
(ii) Partnership deed
(iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf
(iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney, their addresses and their signatures
(v) Telephone bill in the name of firm
(vi) Photo & PAN details of the person holding Power of Attorney
(vii) PAN Card of the partnership frim

iii. Corporate

Information:

(i) Name of the corporate
(ii) Principal place of business
(iii) Mailing address of the corporate
(iv)Telephone/Fax Number

Certified copy each of the following documents:

(i) Certificate of Incorporation – CIN details
(ii) Memorandum & Articles of Association
(iii) List of officials with names, designation and signatures authorized by the Managing Director / Chief Financial Officer / Company Secretary of the company to conduct transactions on behalf of the company
(iv) The PAN details & any OVD's with one recent photograph of Authorised signatories /Promoters/ Ultimate Beneficial Owner
(v) PAN Card of the company
(vi) Address Proof – Latest Electricity bill/Water bill/Land line Telephone bill

iv.Trusts, Societies and Foundations

Information

(i) Names of trustees, settlors, office bearers, beneficiaries and signatories
(ii) Names and addresses of the founder, the managers/directors and the beneficiaries
(iii) Telephone/Fax numbers

One certified copy of each of the following:

(i) Registration certificate & Trust Deed
(ii) PAN card of the trust
(iii) Power of Attorney granted to transact business on its behalf
(iv) Any officially valid document, PAN details & a photograph to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses
(v) Resolution of the managing body of the foundation/ association
(vi) Address Proof – Electricity bill/Water bill/Land line Telephone bill
(vii) List of persons duly authorized to conduct transactions on behalf of the body with names, designation and signatures, attested by the trustees.

We shall ensure that NPOs, as defined in the Master Directions, are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, we shall persuade them to do the registration.

5.2.2. c. Identification of Ultimate Beneficial Owners

While permitting a person to act on behalf of another person/entity, the Company shall identify the beneficial owner as provided for in sub rule (3) of Rule 9 (1A) of PMLA Rules, 2005 and take all reasonable steps to verify his identify. Ultimate Beneficial Owner (UBO) includes Promoters/Shareholders, Directors, Authorised signatories. CDD measures need to be applied for UBO's.

a. Where the customer is a **Company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest more than 10% of the shares/profit or who exercise control through other means.

b. Where the customer is a **Partnership firm/Trust/AoP/BoI**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than the specified per cent of the capital/profits of the entity.

For this purpose, a copy of any OVD containing details of his identity and address, one recent photograph and Permanent Account Number of the beneficial owner are to be obtained and also a copy of any OVD containing details of his identity and address of the person acting on behalf of the beneficial owner i.e. the third party.

Trust/nominee or fiduciary relationship can be used to circumvent the customer identification procedure. In all cases where the customer is acting on behalf of another person as trustee/nominee or any other intermediary, we shall insist for satisfactory document of identity of intermediaries and other persons on whose behalf they are acting. Also, we shall obtain details about the nature of the trust or other arrangements in place. In the case of foundations, steps shall be taken to verify the founder managers/directors and the beneficiaries.

Enhanced due diligence need to be carried out by the company while dealing with the UBO's. Care shall be taken to ensure that trust/nominees or fiduciary relationships are not used as a 'front' for money laundering.

5.2.2. d. Central KYC Registry

In case of establishing an account-based relationship with an individual customer, personal details with Proof of Identification and Address are required to be captured and uploaded under the CKYCR Rules for generation of identifiers. PAN of customers shall be obtained and verified as per the provisions of Income Tax Rule 114B, wherever applicable.

In case of establishing an account-based relationship with a non-individual customer, all the details required by the RBI/CKYCR guidelines like the constitution of the entity, registration, pan, date of incorporation, identification of related persons, etc. with proofs are required to be captured and uploaded under the CKYCR Rules for generation of identifiers.

Where a customer submits a KYC Identifier to open an account, the KYC records shall be retrieved online from the Central KYC Records Registry by using the KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless-

(i) there is a change in the information of the client as existing in the records of Central KYC Records Registry. (ii) the current address of the client is required to be verified; (iii) any requirement is felt in order to verify the identity or address

of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
In case of obtaining any additional or updated information from a customer, it shall as soon as possible be furnished to the Central KYC Records Registry.
KYC records of a customer obtained from the Central KYC Records Registry shall not be used for any purposes other than verifying the identity or address of the client and
shall not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or by the Regulator or by the Director, FIU-India.

5.2.3 Monitoring of Transactions

Monitoring of transactions on an ongoing basis is a key element of KYC procedures so as to have an effective control and to reduce the risk. On-going Due Diligence means regular monitoring of transactions to ensure that customer transactions are consistent with profile of the customer, risk category and the source of fund.

Based on the risk perceptions, care shall be taken to see whether there is any change in the pattern of transactions carried out by the customer and the same is reasonable. Enhanced Due Diligence shall be applied to all complex & unusual patterns inconsistent with the normal and expected activity of the customer which have no apparent economic or visible lawful purpose.

We shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and the purpose of such transactions shall, as far as possible, be examined and written findings together with all the documents shall be retained and made available to RBI/other relevant authorities on request. Necessary limits shall be placed while delegating powers to the officials for handling transactions and cases beyond a particular limit shall be approved by higher officials. The transactions shall be reviewed from time to time, so that merely establishing relationship shall not let the customer out of scrutiny. Additionally, review of risk categorization of customers shall be carried out by the Company from time to time under such periodicities as prescribed by the Regulators.

5.2.3. a. Attempted Transactions

We shall not undertake transactions where we are unable to apply appropriate KYC measures due to reasons such as:
(a) Non-furnishing of or misleading/fake identity info by the customer
(b) Non-co-operation by the customer to reveal background details of the transaction
Such cases shall be reported to the Financial Intelligence Unit – India (the FIU-IND) by way of a STR even if the transaction is not put through. 19

5.2.3. b. Transactions by Politically Exposed Persons (PEPs)
Politically Exposed Persons" (PEPs) are individuals who have been entrusted with prominent public functions at Govt./Judiciary/ Military/ Political Party officials/State-Owned Corporations & Big corporate house in India or abroad. The family members/close relatives of PEP's also shall be considered as PEP. Before accepting PEP as a customer, we shall identify him/her and also find out his/her sources of funds. Such customers shall be subject to enhanced due diligence and shall be dealt with at the level of senior management at HO. Their transactions shall be monitored on an ongoing basis and the above rule shall be applicable even while dealing with the family members or close relatives of the PEPs and also to those who become PEP subsequent to establishing relationship with us as a customer. The decision to continue business relations with such customers would be taken at the level of senior management at HO. Such an exercise shall be carried out to individual transactions/business relationship where a PEP is the ultimate beneficial owner. Further, we have an appropriate ongoing risk management procedure for identifying and applying enhanced CDD to PEPs, customers who are family members or close relatives of PEPs and individual transactions/business relationship of which a PEP is the ultimate beneficial owner.

5.2.4 Risk Assessment & Management – Money Laundering & Terrorist Financing

Keeping in view the objectives of National Money Laundering/Financing of Terror Risk Assessment Committee of Government of India and in compliance with the newly incorporated section 5(a) of chapter II of the Master Direction on KYC, we have adopted a risk based approach for assessment, mitigation and management of the identified risks for customers, countries, geographic areas, products & services and types of transactions undertaken-cash/any monetary instruments/wire transfers/forex transactions, etc.
The system put in place would use the assessment so adopted to take steps to effectively counter money laundering/terrorism finance so as to make AML/CFT regime more robust. We shall allocate resources more judicially and efficiently for the purpose.
Each customer shall be assigned an appropriate risk rating based on his/her profile and enhanced due diligence measures shall be applied to high risk customers. We shall identify and assess money laundering/terrorism finance risk to our customers, countries and geographical areas as also for products/services/transactions/ delivery channels etc.

An effective KYC programme has been put in place by establishing appropriate procedures and ensuring effective implementation covering proper management oversight, systems and controls, segregation of duties, training, and other related matters. Internal control system has been put in place to:
(a) Assess each customer for the risk, assign a risk rating and accordingly undertake due diligence
(b) Approve transactions
(c) Monitor transactions both online (System checks) & offline (Manual Monitoring).

Necessary limits are in place for approval of transactions and all transactions beyond a threshold limit shall be approved at higher levels.
While the online monitoring shall be through the system controls, offline monitoring shall be done by deputing senior officials to the branches to conduct a surprise inspection. This shall be in addition to the Concurrent Audit System already in place. The staff shall be trained and refresher courses shall be conducted to enable them to update their knowledge. The risk profiles of the customers shall be reviewed and updated from time to time.
The mandatory Concurrent Audit is entrusted to independent audit firms with instructions to check all the transactions and to ensure that the transactions are undertaken in compliance with the anti-money laundering guidelines and necessary reports are furnished to the authorities concerned. These reports are provided to the regulators, whenever required

6. Record Management – Maintenance & Destruction

In compliance with the PMLA and the rules made there under, all records of the transactions of the customers, both domestic and international shall be maintained for the period of five years from the date of transaction between the customer and the Company as prescribed under Section 12 of Prevention of Money Laundering Act, 2002 through Prevention of Money Laundering (Amendment) Act, 2012. The records/information shall be retained in hard/soft copy to retrieve the same at a short notice, if required by the law enforcing agencies, regulators etc.

7. Senior Management, Designated Director, Principal Officer (PO) & Alternate PO

Senior Management

The senior management for the purpose of AML/KYC/CFT compliance shall include the Product Heads who is responsible for the activities under various licences, IT leadership, Compliance Head, Audit Head, HR Head, CFO & MD.

The responsibilities of senior management shall be in place for effective implementation of policies and procedures. The prime responsibility of ensuring compliance to KYC policy shall rests with the Product Heads (procurement and verification) & IT shall provide necessary system support to validate and store the information collected from customer. The compliance shall be responsible for designing the system/process and proper guidance based on the regulations issued from time to time. The audit shall be responsible for identifying the gaps/lapses and shall verify the adherence of KYC/AML policies and procedures. HR is responsible for hiring of employees & disciplinary actions against employees. CFO/MD shall be responsible to report to the audit committee/Board.

There shall be periodic independent evaluations of compliance program of company's policies and procedures.

Designated Director

The Company had nominated Mr. Babu Alias, Managing Director on our Board as "Designated Director", as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules.

Principal Officer

The Company had appointed Chief Financial Officer as the Principal Officer (who is also known as Money Laundering Reporting Officer (MLRO). He is in the Senior Management cadre of our Company and shall operate from the Head Office. His roles and responsibilities include overseeing and ensuring overall compliance with regulatory guidelines on AML/CFT/KYC issued from time to time and obligations under PMLA. He shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He shall maintain close liaison with the FIU-India, Regulators like RBI & other Law Enforcement Agencies.

He and his supporting personnel shall have timely access to customer identification data, transaction records and other relevant information. He shall act independently without fear or favour and report to the top management. He shall also be responsible for submission of CTR/STR to FIU-India.

Alternate Principal Officer

We had appointed Ms. Anju B Nair to be the Alternate Principal Officer to take charge of the Principal Officer in the absence of the latter.

8. Escalation of Suspicious Activity

All branch heads are by default the compliance officer of that location. The branch staff and agents mapped to the branch must report the transactions of suspicious nature to the Compliance Officer (Branch Head) on the following grounds

a) Address provided by the customer is found to be non-existent or Customer frequently requests for change of address.

b) Customer is reluctant to provide details/documents on frivolous grounds

c) KYC documents presented by the customer are not verifiable & false identification documents.

d) Different OVD's are produced on different occasions, to avoid linkage of multiple transactions.

e) Customer approaching for transacting business beyond banking hours or on bank holidays and requesting for acceptance of cash in excess of the permissible limit on the grounds of non-availability of banking facilities with a promise to get the cash exchanged for cheque/demand draft at a later date

f) Common address & phone nos used by multiple unrelated customers

g) Customer uses complex legal structures or where it is difficult to identify the beneficial owner while on-boarding.

h) Customer is dealing with complex equipment's for which they lack knowledge & engages in complex trade deals (third parties)

i) Repeated or large transfers from or to high-risk jurisdictions, countries with political unrest or instability.

j) Money transfer to a location prior to or immediately after a terrorist incident.

k) Signs of confusion and nervousness appear on the customer during the execution of the operation and Customer could not explain source of funds satisfactorily.

l) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.

m) Transactions conducted with persons/entities that have no clear connection with the customer.

n) Transactions with several persons without clear justification especially if they are of different nationalities.

o) The transfer of repeated or large amounts to persons in a region reputed for criminal activity.

p) Transferring funds to a number of persons in different countries without a justification.

q) The value of transactions does not match the information available on the customer, his activity, income & lifestyle.

r) Transactions in a series are structured just below the regulatory threshold to avoid EDD or regulatory reporting.

s) Any other transactions which the branch/agent feels is suspicious in nature or has relevant information that it is proceeds of crime.

The Branch Head (Compliance Officer) analyses the transactions reported by the counter staff and escalate the same to PO/MLRO of the company.