

KYC/AML/CFT/OBLIGATION OF BANKS UNDER PMLA 2002

The objective of Know Your Customer (KYC) norms/ Anti-Money Laundering (AML) Measures/ Combating of Financing of Terrorism (CFT) guidelines is to prevent the banks being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. The KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

Know Your Customer (KYC)

A 'Customer' is defined as :

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

Guidelines – General

- The information collected from customers for the purpose of opening of account is to be treated as confidential and should not be divulged for cross selling or any other purposes.
- Remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rs. 50,000/- and above is effected by debit to the customer's account or against cheques and not against cash payment.
- Banks shall not make payment of cheques/drafts/pay orders/banker's cheques bearing that date or any subsequent date, if they are presented beyond the period of **three months** from the date of such instrument (w.e.f. 01.04.2012)
- Banks are required to ensure that the provisions of Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

KYC Policy

Banks are required to frame their KYC policies incorporating the following four key elements:

- i) Customer Acceptance Policy;
- ii) Customer Identification Procedures;
- iii) Monitoring of Transactions; and

iv) Risk Management.

i) **Customer Acceptance Policy (CAP)**

- a) Every Bank has to develop their CAP with explicit criteria for acceptance of customers. The CAP must ensure that explicit guidelines are in place covering various aspects as under:-
- No account is opened in anonymous or fictitious/benami name/s.
 - Parameters of risk perception in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. should be defined for categorization of customers into low, medium and high risk.
 - Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Customers that are likely to pose a higher than average risk to the bank should be categorized as medium or high risk

Example: Low Risk Category :

Salaried employees, people belonging to lower economic strata of the society, Government Departments and Government owned companies, Regulators and Statutory bodies, NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers, etc. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

Medium/High Risk Category :

- Non-resident customers,
 - High net worth individuals,
 - Trusts, charities, NGOs and organizations receiving donations
 - Companies having close family shareholding or beneficial ownership
 - Firms with 'sleeping partners'
 - Politically exposed persons (PEPs) of foreign origin
 - Customers (who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner)
 - Non-face to face customers; and
 - Those with dubious reputation as per public information available, etc
- Banks should apply enhanced due diligence measures based on the risk assessment especially those for whom the sources of funds are not clear.

- Documentation/information requirements to be collected from different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by RBI from time to time.
- Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures including verification of identity/intention of required documents, etc.
- 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 and practice of banking.

- Cross verification of identity of customers that does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.

b) Banks may prepare a profile for each new customer based on risk categorization with relevant information relating to customer's identity, social/financial status, nature of business activity, details of his clients' business and their location etc. This information is to be treated as confidential.

- c) The customer acceptance policy should not be too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

ii) **Customer Identification Procedures (CIP)**

- Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.
- The Policy approved by the Board should explicitly spell out the Customer Identification Procedure to be carried out at different stages.
- Banks need to obtain such information that are sufficient to establish to their satisfaction the identity of each new customer irrespective of the nature/status of the people and taking into account the risk perception involved.
 - Banks need to introduce a Unique Customer Identification Code (UCIC) for each customer to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable them to have a better approach to risk profiling of customers. For existing customers, allotment of UCIC has to be completed by 31.12.2014.
- In case of any room of 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, banks may carry out full scale customer due diligence (CDD) before opening an account. In case of an existing customer in case of suspicion, banks shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.
- In case of close relatives e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, find difficult to open an account for want of address verification, Banks can open account by obtaining an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her.
- It is necessary to provide only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation.
- Banks may transfer existing accounts at the transferor branch of the bank to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address.

- Banks should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updating may be once in **ten years** in case of low risk category customers, once in **eight years** in case of medium risk categories and every **two years** in case of high risk categories customers. Positive confirmation (obtaining KYC related updates through e-mail/ letter/ telephonic conversation/ forms/ interviews/ visits, etc.), may be completed at least every **two years** for medium risk and at least every **three years** for low risk individuals and entities.
- An indicative list of the nature and type of documents/information that may be relied upon for customer identification is annexed to RBI Master Circular dt. 01.07.14.

Customer Identification Requirements (Indicative)

a) Walk-in Customers

- Transaction/s for amount equal to or exceeds Rs. 50,000/- by a walk in customer (non-account holder) whether constructed as a single transaction or several transactions, the customer's identity and address should be verified. In case bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank may verify identity and address of the customer and also may consider filing a suspicious transaction report (STR) to FIU-IND.
- Banks/FIs are required to verify the identity of the customers for all international money transfer operations (Rule 9 of the PML Rules 2005)

b) Salaried Persons

For salaried employees, banks can rely on certificate/letter of identity /address issued only from corporate and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter and additionally insist for at least one of officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving licence, PAN Card, Voter's Identity card, etc.) or utility bills for KYC purposes for opening bank accounts.

c) Trust/Nominee or Fiduciary Accounts

While opening an account for a trust, banks are required to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. In case of Foundation, steps should be taken to verify the founder managers/directors and in both the cases the beneficiaries should be identified, if defined.

d) Accounts of companies and firms

Banks need to examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

e) Client accounts opened by professional intermediaries

- If the account is opened for a single client by the professional intermediary, the client must be identified. In case of 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds and accounts managed by Lawyers/CAs or Stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients, and the funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified.
- Banks should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality.

f) 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.
- Banks need to verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer and the decision to open an account for PEP may be taken at a senior level as per the Customer Acceptance Policy. Such accounts are subject to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.
- Decision on continuance of an existing account for having becoming the account holder a PEP is to be taken at Senior level and the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.
- Further, banks are required to have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner.

g) Accounts of non-face-to-face customers

In case of non-face-to face customers, banks have to insist for certification of all the documents presented and if necessary additional documents may be called for. First payment to be effected through another bank which adheres to similar KYC standards. In the

case of cross-border customers, the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

h) Accounts of proprietary concerns

Banks, besides the extant guidelines on customer identification procedure as applicable to the proprietor, insist for any two of the documents in the name of the proprietary concern viz.a) Proof of the name, address and other documents evidencing the activity of the concern viz. registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, etc.

i) Operation of bank accounts & money mules

In order to minimize the operations in mule accounts as also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters, it has been directed that Banks should follow meticulously the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened.

j) Bank no longer knows the true identity

In the circumstances when a bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the bank should also file an STR with FIU-IND.

k) Accounts with Introduction

In case of low income group persons both in urban and rural areas who find it difficult to produce the documents for identification and address, the banks may consider opening of Small Deposit Accounts based on the introduction from another account holder who has been subjected to full KYC procedure and his account is at least six months old and show satisfactory transactions. The maximum balances **not exceeding Rs. 50,000/-** in all their accounts taken together and the total credits in all the accounts taken together are not expected to **exceed Rs. 1 Lac** in a year. The address needs to be certified by the introducer, **or** any other evidence as to the identity and address of the customer to the satisfaction of the bank.

l) Accounts of foreign students:

- Banks may open Non Resident Ordinary (NRO) on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.
- Obtaining a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility within a period of 30 days of opening the account

- During the period the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.
- On submission of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the RBI instructions on NRO account and FEMA guidelines.
- Students with Pakistani nationality will need prior approval of RBI for opening the account.

m) Small Account

Small Accounts are accounts wherein:-

- i) the aggregate of all credits in a financial year does **not exceed rupees one lakh**;
- ii) the aggregate of all withdrawals and transfers in a month does **not exceed rupees ten thousand**; and
- iii) the balance at any point of time does **not exceed rupees fifty thousand**.

For opening of accounts, banks may accept **job card issued by NREGA** duly signed by an officer of the State Government or **letters issued by the Unique Identification Authority of India** containing details of name, address and Aadhaar number, etc. as documentary evidence of identification and proof of address.

iii) **Monitoring of Transactions**

Every bank has to set key indicators for accounts taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. High risk associated with accounts of bullion dealers (including sub-dealers) & jewellers should be taken into account by banks to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND).

Banks are required to have in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers should be carried out at a periodicity of **not less** than once in six months.

Banks are required to exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds

Closure of accounts

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank may consider closing the account or terminating the banking/business relationship after issuing due notice to the

customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

iv) **Risk Management**

- The Board of Directors of the bank are expected to ensure that an effective KYC programme covering proper management oversight, systems and controls, segregation of duties, training and other related matters is put in place by establishing appropriate procedures and ensuring their effective implementation. Responsibility should be explicitly allocated within the bank for ensuring effective implementation of the policies and procedures.
- Banks are expected to ensure that its internal audit and compliance functions should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.
- Banks are expected to ensure that preventive measures are put in place to take care of the money laundering threats that may arise from new or developing technologies including internet banking. Banks should ensure that full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. It is also desirable that Marketing Agents of these products are also subjected to KYC measures.

Combating Financing of Terrorism

- Any transaction which gives rise to a reasonable ground of suspicion that may involve financing of the activities relating to terrorism is to be treated as suspicious transaction (PMLA rules). Banks need to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.
- RBI provides list of individuals and entities having terrorist connections periodically. Banks/Financial Institutions are required to update the consolidated list of individuals and entities as circulated by RBI. Banks may scan its existing portfolio to ensure that no account is held by or linked to any of the entities or individuals included in the list as also before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

- Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or

entities or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities or any other person engaged in or suspected to be engaged in terrorism (Sec. 51A of UAPA)

- Banks are required to strictly follow the procedure laid down in the UAPA Order and ensure meticulous compliance.
- Banks have to maintain the list of individuals or entities in electronic form and run a check on the given parameters and in case the particulars match with any of its existing customers, the banks shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, by Fax and also convey over telephone followed by post and e-mail duly marking copy to the UAPA nodal officer of RBI, CGM, DBOD, RBI (AML Division).
- Banks shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (b) above, carried through or attempted, as per the prescribed format.

Freezing of financial assets

- On receipt of the particulars from Bank/FI, the MHA would get the veracity of the data verified by State Police and /or the Central Agencies. The verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.
- In case of positive findings, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to Reserve Bank of India and FIU-IND. The order shall take place without prior notice to the designated individuals/entities.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons or entities figured in the list. Any requests under the Resolution would be acted upon by the Ministry of External Affairs and passed on to RBI who in turn forwards the same to the concerned bank/s for freezing of the assets.

Procedure for unfreezing of financial assets inadvertently affected

Any application for release of inadvertent freezing of assets would be attended to by Ministry of Home Affairs (MHA) and if found satisfied suitable order would be passed for unfreezing the assets within 15 working days under intimation to the concerned bank through RBI.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

- Banks are required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the **Financial Action Task Force (FATF)** and should also give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations.
- If the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

Correspondent Banking

Correspondent banking is the provision of banking services viz. cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Prior to establishing such relationships, Banks are required to carry out due diligence by collecting various information including level of AML/CFT compliance, whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action, etc. Proper approval of the Board or committee headed by the CMD/CEO is desirable.

Correspondent relationship with a “Shell Bank”

A Shell Bank is one which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. Shell banks are not permitted to operate in India. Banks shall not enter into relationship with shell banks and ensure that its foreign respondent institution does not permit its accounts to be used by shell banks.

Applicability to branches and subsidiaries outside India

The guidelines on KYC/AML/CFT would apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. Any deviation to the RBI guidelines should be reported to RBI. In case there is a variance in KYC/AML standards prescribed by RBI and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

Wire Transfer

- Wire transfer is a transaction carried out on behalf of an originator (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. Cross-border wire transfer means where the originator and the beneficiary bank or financial institution are located at different countries whereas domestic wire transfer where the originator and beneficiary are located

in the same country. It is an expeditious method for transferring funds between bank accounts.

- Basic information on the originator of wire transfers should be made available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary. Banks must ensure that all wire transfers whether cross-border or Domestic must be accompanied by the originator information.
- Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements

Mandatory information

a. Cross broader wire transfer

- i) Accurate and meaningful originator information
- ii) Name and address of the originator
- iii) Number of that account, if account exists
- iv) Unique reference number, in the absence of account
- v) Bundled in a batch file for transmission only Unique reference number of the country be insisted upon.

b. Domestic Wire transfer

Originator information i.e. name, address and account number etc. in case the transfer of Rs. 50000/- and above.

Maintenance of records of transactions (Rule 3 of PML Rules, 2005)

Banks are expected to maintain:-

- a) All cash transactions of the value of **more than Rs. 10 Lakh** or its equivalent in foreign currency;
- b) All series of cash transactions integrally connected to each other which have been valued **below Rs. 10 Lakh** or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceed Rupees Ten Lakh;
- c) All transactions involving receipts by non-profit organizations of value **more than Rs. 10 lakh** or its equivalent in foreign currency
- d) All cash transactions wherein forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and
- e) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- f) All integrated transactions **exceeding Rs. 10 Lakh.**

Information to be preserved

Banks are required to maintain information in respect of the **above transactions** as under:-

- a) The nature of the transactions;
- b) The amount of the transaction and the currency in which it was denominated;
- c) The date on which the transaction was conducted; and
- d) The parties to the transaction

Maintenance and Preservation of record

Banks are expected to maintain/preserve records for at least **five years** from the date of transaction between the bank and the client all necessary records of transactions, both domestic or international including records pertaining to the identification of the customer and his address which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

Records relevant to identification of the customer and his address are to be preserved for at least **five years after the business relationship is ended.**

Reporting to Financial Intelligence Unit - India

Banks are required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organizations of value more than Rs. 10 lakh or its equivalent in foreign currency to the Director, FIU-IND (PMLA Rules).

FIU-IND has released a new single XML file format for reporting by banks. Detailed guidelines have also been issued by FIU-IND for reporting. Banks are required to prepare a profile for each customer based on risk categorization and undertake review of the same periodically.

Customer Education/ Training of Employees / Hiring of Employees

Customer Education

Banks are required to introduce suitable means to educate the customers of the objectives of the KYC programme so as to avoid any resistance from the customers.

Training of Employees

Banks must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures.

Hiring of Employees

Banks are required to put in place adequate screening mechanism as an integral part of their recruitment/hiring process of personnel so as to ensure that criminals are not allowed to misuse the banking channels.

(List of documents that are to be obtained from customers for customer identification)

purpose is given in detail in the circular)

(Source: RBI M. Cir. Dt.01.07.14)

o0o0o0o0o

GURUJI24.COM