

R Gandhi: KYC – compliance vs convenience

Speech by Mr R Gandhi, Deputy Governor of the Reserve Bank of India, at the Federation of Andhra Pradesh Chambers of Commerce and Industry, Hyderabad, 23 May 2014.

* * *

Assistance provided by Shri Thomas Mathew, General Manager is greatly acknowledged.

Is KYC a recent phenomenon?

KYC was always there in banking! The focus, earlier, was more on the asset side and not on the liability side as no banker could risk parting with his funds to an unknown person. The thorough appraisal process to screen the potential borrowers is a good example of KYC process.

Then, issues such as illegal/black money and more recently, terrorism financing became matters of serious concern and then KYC on payments and remittances, and consequently on the liability side (deposit accounts, etc.) started assuming high importance.

Why KYC/AML norms

Sound KYC policies and procedures are critical for protecting the safety and soundness of banks and the integrity of banking system in the country.

Due to increasing globalisation of Indian banks, their interaction with other countries' financial systems are expanding, making the task of ensuring safety of our systems more critical. International obligations and inter-regulatory consensus built via United Nations Resolutions, Basle Committee on Banking Supervision and the Financial Action Task Force also require that we put in place an elaborate KYC Framework in India.

Financial Action Task Force (FATF)

The FATF is an intergovernmental body established in 1989 (G-7 initiative). Its tasks are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. It is a policy-making body which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. It monitors the progress of its members in implementing necessary measures. There are 36 full-fledged members. India is one of them. Over 18 jurisdictions around the world have committed to the FATF Recommendations. India has also committed to implement the recommendations of FATF. Originally, in 1990, FATF had 40 recommendations focussing on drug money. It revised its recommendations in 1996 and broadened the scope. Then in 2001, it added eight (later nine) special recommendations to combat financing of terrorism which were further revised in 2003. The latest exercise in 2012 had further revised the recommendations and combined the 40+9 to 40.

Basel Committee

Findings of an internal survey of cross-border banking in 1999 by the Basel Committee identified deficiencies in KYC policies for banks in a large number of countries. It constituted a Working Group on Cross-border Banking to examine the then KYC procedures and to draw up standards applicable to banks in all countries. It issued a consultative document, called the Customer Due Diligence for banks (CDD) in January 2001. While the FATF's focus is on money-laundering and terrorist financing, the Basel Committee's approach to KYC is from a

wider prudential, and risk-management perspective, not just anti-money laundering perspective.

PMLA – Salient features

UN General Assembly resolution (1990) calls upon the Member States to adopt national money-laundering legislation and programme. Accordingly, in India the Prevention of Money Laundering Act (PMLA), 2002 was enacted in January 2003. The Act along with the Rules framed there under has come into force with effect from 1st July 2005.

The objectives of the PMLA are to:

- prevent and control money laundering
- confiscate and seize the property obtained from the laundered money
- prescribe fines and penalties for offence

The important feature of the Act is that the burden of proof is on the accused.

Regulatory stance

The Reserve Bank's regulatory stance on KYC is with the aim to safeguard banks from being used by criminal elements for money laundering activities and to enable banks to understand the risk posed by customers, products and services, delivery channels and helping them assess and manage their risks prudently. At the same time, the Reserve Bank is fully conscious that the KYC framework will have to be relevant to the perceived risk and not intrusive in nature nor too strict resulting in denial of banking services to general public.

As far as Indian banking sector is concerned, some of the initial steps taken (instructions issued) in respect of KYC are as under. Actually these instructions are there for the past 50 years or so, as far back as from 1965.

- 1965 – Banks were asked to ensure that full and correct addresses of the depositors are recorded (Benami accounts & avoidance of tax).
- 1976 – For opening of accounts, in order to establish the identity of account holders/avoid benami accounts, the concept of "Introduction" was prescribed.
- 1987 – There should be reasonable gap of say, 6 months between the time an introducer opens his account and introduces another prospective account holder to the bank. Introduction of an account should enable proper identification of the person opening an account so that the person can be traced if the account is misused.
- 1991 – No cash transaction above ₹ 50,000/ – for TCs/ DDs/MTs/TTs
- 1993 – Banks to keep vigil over heavy cash withdrawals by account holders which may be disproportionate to their normal trade/business requirements and cases of unusual trends
- The banks to introduce the practice of obtaining photographs of the depositors/account holders who are authorised to operate the said accounts at the time of opening of all new operative accounts with effect from 1st January 1994
- 1995 – Monitoring & special reporting for cash transactions of value more than ₹10 Lakh.
- 1999 – Confirmation by post from both the customer and the introducer before issue of cheque book
- 2002 – KYC circular

Paradigm shift – KYC prior to & post Nov’ 04

After the international focus on KYC, the Reserve Bank brought on a paradigm shift in the approach to KYC by banks in India. It moved away from introduction to document based identification – hence introduction not required. It also shifted the focus from financial loss (from frauds) to the banks to the loss of reputation to the banks (by non-compliance). The other principles are that the KYC information collected is to be consistent with risk perception and other information to be collected only with consent of the customer and the KYC related information is confidential – not to be divulged for cross-selling or any other purpose.

Regulatory prescriptions

Who is a Customer – a KYC context

In the context of KYC framework, the concept of “customer” has now been redefined. A “customer” is no longer just the one who has an Account and/or business relationship with the bank; the ones on whose behalf the account is maintained (i.e. the beneficial owner), the beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors and any person/entity connected with any financial transaction which can pose risk to bank, say, through a wire transfer/issue of a high value DD, etc are all “customers”.

KYC policy of banks – the 4 key elements

The Reserve Bank has prescribed that the KYC policy of banks should have the following key elements:

- i) Customer Acceptance Policy
- ii) Customer Identification Procedures
- iii) Monitoring of Transactions, and
- iv) Risk Management

Customer acceptance policy

The salient features are:

- No anonymous or fictitious/benami accounts to be allowed
- Not to open/close accounts when unable to apply appropriate Customer Due Diligence (CDD – decision to close a/cs to be taken at reasonably high levels after issuing due notice to the customers).
- Define parameters of risk perception to enable categorisation of customers
- Documentation/information requirements for different risk categories (to prepare a profile of each customer)
- Circumstances where a customer is permitted to act on behalf of another person/entity, should be spelt out (eg., account is operated by a mandate holder)
- Identity of the customer does not match with those of criminal backgrounds/banned entities (terrorists, etc.)

Customer Identification Procedures (CIP)

- Customer identification – identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.

- The banks must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.
- Such risk-based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers.
- Nature of information/documents required would also depend on the type of customer (individual, corporate etc.)

CIP – When customer ID is required

- While establishing a banking relationship
- While carrying out a financial transaction as in the case of a “Walk in Customer”
- When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data

CIP – PMLA requirements

- Banks to obtain “Officially Valid Documents (OVD)”.
- OVDs are “Passport, Driving License, the Permanent Account Number (PAN) Card, the Voter’s Identity Card issued by the Election Commission of India; UIDAI letter containing name, address and Aadhaar number and NREGA Card duly signed” or any other document as may be notified by the Central Government.
- When there are suspicions of money laundering or financing of the activities relating to terrorism/ there are doubts about the adequacy or veracity of previously obtained customer identification data, banks should review the due diligence measures including verifying again the identity

Banks are required *to verify the identity of the customer for all international money transfer operations*

CIP – Natural Persons (NP) – Identification documents

- PAN card, Passport, Voter’s Identity Card, Driving license, UIDAI Letter – Aadhaar, NREGA Card duly signed by an officer of State Govt.
- Identity card issued by employer (subject to the bank’s satisfaction)
- Letter from a recognized public authority or public servant verifying the id & address (subject to the bank’s satisfaction)
- Salaried employees – letter of identity and/or address from corporates and entities of repute (1 officially valid document is required).

CIP – NP – Address documents

- Telephone bill
- Bank account statement
- Letter from any recognized public authority
- Electricity bill
- Ration card

- Letter from employer (subject to satisfaction of the bank) if an officially valid document is produced for identity
- Rent agreement duly registered with state Govt or similar Regn. Authority indicating the address of the customer.
- Based on self-declaration, accounts could be transferred from one branch to another without address proof (correct address proof is to be obtained by the transferee branch within 6 months).
- Any one of the documents would suffice (If address is available in ID document, single document is sufficient).
- Banks to obtain sufficient information necessary to establish, to their satisfaction, the identity of customer and the purpose of the intended nature of banking relationship.
- Banks need to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer.
- Banks have been advised to accept e-KYC service of UIDAI as a valid process for KYC verification. The information including the photographs made available from UIDAI as a result of e-KYC process to be treated as “Officially Valid Documents”.

CIP – Close relatives

- In respect of close relatives, e.g. wife, son, daughter and parents, etc who live with their husband, father/mother and son, etc., banks can obtain 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.
- Banks can use any supplementary evidence such as a letter received through post for further verification of the address.

CIP – PEPs (non-resident)

Politically Exposed Persons (PEPs) are individuals who are entrusted with prominent public functions in a foreign country (as of now, we are focusing on foreign PEPs). e.g., Heads of states/Govts., senior politicians, senior Govt/judicial/defence officers, senior executives of state-owned corporations

- Banks to compile all information, identity details, and details of sources of funds before accepting a PEP as customer
- Decision to open account for PEPs to be taken at a senior level as spelt out in the policy.
- Family members and close relatives of PEPs are also to be subjected to same CDD

CIP – Non face-to-face customers

Apart from applying the usual customer identification procedures, the following are to be taken care of:

- Certification of all the documents presented
- First payment to be effected through the customer’s account with another bank with similar KYC standards.
- In the case of cross-border customers involving third party certification/introduction of the customer, the third party is to be a regulated and supervised entity.

CIP – Unique Customer Identification Code (UCIC)

- Need to ensure that customers do not have multiple identities within a bank, across the banking system and across the financial system
- The UCIC will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers.
- Central KYC registry is under consideration

CIP – Legal Persons (LP)

- Verify the legal status of the legal person/ entity through proper and relevant documents
- Verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person
- As per PML Rules, beneficial person should be identified by banks/FIs
- Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person

CIP – LP – Beneficial owners

Beneficial owner is the natural person who ultimately owns or controls a client and/or the person on whose behalf transaction is being conducted. Includes a person who exercises effective control over a juridical person.

- Controlling ownership – Companies >25% shares/capital/profit; Partnership >15% of capital/profit; Unincorporated association/body of individuals > 15% of property/capital/profit; Trust > = 15% interest in Trust/Settler of Trust/Anyone exercising effective control over Trust.
- In case of companies, partnerships, associations, etc., if no natural person could be identified as above, the senior managing official would be reckoned as BO.
- Where the client or the owner of controlling interest is a company listed on stock exchange/majority owned subsidiary of such a co., not necessary to identify the BOs of such companies.

CIP – Legal persons – companies

Copies of the following documents would be required:

- Certificate of incorporation and Memorandum & Articles of Association
- Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account
- Power of Attorney granted, if any
- Copy of PAN allotment letter

CIP – LP – Partnership firms

Copies of the following documents would be required:

- Registration certificate, if registered
- Partnership deed

- Power of Attorney granted
- Any officially valid document identifying the partners and the PA holder and their addresses

CIP – LP – Trusts & foundations

Documents required are:

- Certificate of registration, if registered
- Trust deed
- Power of Attorney granted
- Any officially valid document to identify the trustees, settlors, beneficiaries, PA holder and their address

CIP – Proprietary concerns

- Registration certificate (in case of a registered concern)
- Certificate/license issued by the Municipal authorities under Shop & Establishment Act,
- Sales and Income Tax returns, CST/VAT certificate
- License issued by the registering authorities like ICAI, ICoAI, Institute of Company Secretaries, Indian Medical Council, Food and Drug Control Authorities, etc.
- Complete Income Tax return (not just the acknowledgment) in proprietors name reflecting income from proprietary concern, duly authenticated/acknowledged by IT authorities.
- Utility bills such as electricity, water and landline telephone bills

Customer profile & risk categorization

Banks can effectively monitor, control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. Accordingly, banks are required to build the profile for each customer based on risk categorisation. The parameters of risk perception are: nature of business activity, location of customer and his clients, mode of transactions, volume of turnover and the social and financial status of the customer.

What is risk perception of customers and how it is linked to KYC?

An important feature of the current KYC regime is to obviate disproportionate cost to banks and burdensome regime for the customers. This is ensured by putting in place a risk graded CDD procedure, say: Low Risk, Medium risk and High Risk and appropriate CDD level accordingly. Is risk categorisation a one-time affair? No. It will be an ongoing affair and banks should have a system of periodical review of risk categorization of accounts once in six months. They have to apply enhanced due diligence measures in case of risk upgradation, which depends on customer transactions/change in profile.

Banks were required to complete the process of risk categorization and compiling/updating profiles of all of their existing customers by end-March 2013. Periodic updation of customer identification data – 2 & 10 years for high and low risk respectively has also been prescribed.

Who are the Low Risk Customers? Typical examples are the salaried employees; accounts with small balance and low turnover; Govt. Deptts. & Govt. owned companies; regulatory and statutory bodies, etc. Who will be the High Risk Customers? They are such as the non-resident customers; HNIs; trusts, charities, NGOs and organizations receiving donations; companies having close family shareholding or beneficial ownership, firms with “sleeping partners”; politically exposed persons; non face-to-face customers, jewellers/dealers in gold bullion and those with dubious reputation as per public information available, etc.

Can a bank refuse to open an account or decide to close an existing account? Yes. When the bank is unable to apply appropriate customer due diligence measures, i.e., Bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the bank. Decision to close an account at high level after due notice to the customer.

Monitoring of transactions

Banks are required to 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. Banks are also required to prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Banks have to particularly guard against the Money Mules – the innocent recruits or persons with fake documents.

Suspicious transactions

Transactions falling outside the regular, normal and reasonable pattern of activity of the customer will be regarded as suspicious transactions. Unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose in regard to customer’s proclaimed business/income activity and transactions that involve large amounts of cash, inconsistent with the normal and expected activity of the customer will qualify to be suspicious transactions. Banks are required to be vigilant about these transactions.

As per PMLA, Suspicious Transactions are that which:

- gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- appear to be made in circumstances of unusual or unjustified complexity; or
- appear to have no economic rationale or bonafide purpose or
- raise suspicions involving financing of terrorism.

Hence, the banks are required to prescribe threshold limits for a particular category of accounts, to pay special attention to the transactions which exceed these limits and 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.

Banks are required to report such transactions (STRs) as per definition in PMLA.

Combating financing of terror

Banks are to develop suitable mechanism for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-Ind on priority. STRs should include suspected cases of terrorist financing. Banks have to be particularly aware of the UNSCR enlisted individuals and entities and accounts and transactions are to be monitored vis-à-vis the list. Any matching found is to be advised to MHA (UAPA – Section 51A).

Unlawful activities (prevention) Act, 1967 (UAPA)

Govt is empowered to freeze, seize or attach funds/financial assets of persons engaged in or suspected to be engaged in terrorism. Under UAPA, RBI forwards the list of individuals/entities subject to UN sanctions to banks. Banks are required to ensure expeditious & effective implementation of the procedure of UAPA for freezing/unfreezing of financial assets.

Financial Intelligence Unit (FIU)

FIU-India has been set up pursuant to PMLA. This is a central agency to collect, collate and analyze financial information. It also disseminates information to concerned investigating authorities, if need be. It receives CTR/STR from banks/FIs and from entities regulated by SEBI/IRDA.

The following types of transactions are to be reported to FIU-IND:

- All cash transactions of the value of more than ₹ 10 Lakh or its equivalent in foreign currency
- All series of cash transactions integrally connected to each other amounting to ₹ 10 Lakh in a month
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or forgery of valuable security or document has taken place
- All suspicious transactions whether or not made in cash
- All receipts by Non-Profit Organizations (NPOs) of ₹ 10 Lakh and above
- Cross-border Wire Transfer Report (CWTR) is required to be filed by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

Customer convenience

We are aware of the possibility that some of these guidelines can be irritating, burdensome to comply with. Several representations and feedback were received to that effect as well. The Reserve Bank therefore periodically reviews these instructions and modifies them, with a view to reduce the burden and bring in ease of compliance, but at the same time ensuring the safety of the financial system and the sanctity of financial transactions are not compromised.

Some of these modifications and adjustments are as follows:

- Any one of the various documents listed would suffice for the identification and address purposes ie one for identification and another one for address; If address is available in ID document, single document is sufficient.
- e-KYC service of UIDAI as a valid process for KYC verification. The information including the photographs made available from UIDAI as a result of e-KYC process to be treated as “Officially Valid Documents”.
- In respect of close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, etc., banks can obtain 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.

- Banks can use any supplementary evidence such as a letter received through post for further verification of the address.

Financial inclusion

We faced challenges in promoting financial inclusion with this KYC framework. Many of the financially excluded may not have proper official document, especially that of address as in the case of migrant people.

As per Customer Acceptance Policy guidelines, the CAP and its implementation should not be too restrictive, and must not result in denial of banking service to public, especially to those who are financially or socially disadvantaged. Banks have been advised not to deny public access to banking services, taking the indicative list of documents as an exhaustive list.

What could be done if required documents are not available?

We have special provision for close family members as mentioned earlier. Small Accounts could be opened by those who do not have the prescribed documents. Small Accounts can be opened with a form filled up & signed before the bank officer with self-attested photograph – bank officer to certify. The small accounts will have the following features: they will have limitations on credit/debit/balance; will be available only at CBS-enabled branches; no foreign remittances will be permitted; will be available only for 12 months – further extension on application for Officially Valid Document; the aggregate of all credits in a financial year does not exceed ₹ One lakh; the aggregate of all withdrawals and transfers in a month does not exceed ₹ ten thousand, and the balance at any point of time does not exceed ₹ fifty thousand.

Additional documents + AEPS

- Documents such as Aadhaar letter & NREGA Card are officially valid documents for identity and address proof.
- **Aadhaar Enabled Payment System** or **AEPS** developed by National Payments Corporation of India allows a person with an Aadhaar number to carry out financial transaction on a Micro-ATM provided by the Banking correspondent.
- With AEPS, the account holders will be able to make balance enquiry, cash withdrawal, cash deposit and Aadhaar to Aadhaar funds transfer.

To conclude

Do we need such elaborate structure? Is it not taking the question of safety too far? Are we paranoid about terrorism and money laundering? Why we have to put ordinary customers of banks to such greater and deeper requirements?

These are legitimate questions that can arise in your mind. But, we have to remember that we are responsible citizens; we have to not only abide by the law, but also help enforcing the law. We are also a responsible nation among the international community. We have obligations to the rest of the world as well.

This KYC structure built by us is not of our own only; it is based on the consensual approach by all the committed nations. It is for the general good of the citizens of the world.

We seek the understanding and the cooperation of all bank customers in complying with the KYC requirements on an ongoing basis. No security comes free of cost or inconvenience. That said, it will be our continued endeavour to minimize such cost and inconvenience. Reserve Bank is committed to ease of operations by bank customers, while requiring the banks to be vigilant about nefarious designs of anti-social elements and terrorists to use the banking and financial systems.