

*ABRIDGED VERSION ON THE POLICY ON
COMBATING FINANCIAL CRIMES*



BANK'S POLICY ON COMBATING FINANCIAL CRIMES

The policy provides the framework for implementation of “Know Your Customer” standards, “Anti Money Laundering / Combating Financing of Terrorism” and other Financial Crimes like ‘Sanctions’, ‘Anti Bribery and Corruption’ and ‘Weapons of Mass Destruction’ to align the Banking operations with good international and industry practice through a proportionate risk-based approach.

The objectives are:

- i. To prevent the Bank’s business channels/products/services from being used as a channel for any financial crime.
- ii. To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Bank.
- iii. To ensure compliance with the laws and regulations in force from time to time.
- iv. To assist law enforcement agencies in their effort to investigate and track money launderers.
- v. To lay down AML compliance norms for the employees of the Bank and to ensure that the relevant staff are adequately trained in procedures to combat Financial Crimes.

Bank will accept only those customers whose identity is established by conducting Customer Due Diligence (CDD) appropriate to the risk profile of the customer

Customer Due Diligence

Customer Due Diligence means identifying and verifying the Customer and Beneficial Owner. Each new individual customer will be accepted for Banking relationship after application of customer due diligence (CDD) measures such as verification of identity, address, nature and location of business activity/profession, purpose of intended Bank account, social and financial status, source of funds etc.

Due diligence includes collection of KYC documents and other information like client profile and purpose of relationship

- i. Verification/Authentication of KYC document/information.
- ii. Identification of ‘Beneficial Owner’ for non-individual customers.
- iii. Collection/Verification of additional information for Enhanced due diligence for High-risk Category of customers.
- iv. Collection/Verification of transactional details.
- v. In case of Bank obtaining Permanent Account Number (PAN) or an equivalent e- document the verification of PAN/digital signature shall be done from the issuing authority/ as per the provisions of the Information Technology Act, 2000 respectively.

Due diligence is conducted while opening the first:

- i. Current Account including collection/escrow account or
- ii. Savings Account or
- iii. Deposit Account or
- iv. Issuance of Credit /Debit/ Prepaid Card or
- v. Walk- in customers/occasional transactions above Rupees INR 50000/- or

- vi. Borrowers/Co-obligants/Guarantors without any liability product

Once the CDD of the customer is complete for any liability/asset account or product or service, as mentioned above, no separate CDD is required for any other account/product/service, unless the subsequent account/product/service specifically mandates fresh CDD, or the existing CDD document/data expired/exchanged, or the client risk categorization changed from Low to Medium/High or from Medium to High and enhanced due diligence is warranted. In case of opening of DEMAT accounts, 'in person' verification shall be recorded and filed in addition to the KYC documents.

While undertaking customer identification, Bank will ensure that:

- i. Introduction shall not be sought while opening accounts.
- ii. While seeking personal information about the customer for evaluating the risk attached with the customer, care will be taken so that only information relevant to risk perception will be sought.
- iii. The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Officially Valid Document (OVD)

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

Where the OVD presented by a foreign national does not contain the details of the address, in such case the document issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address

The documents mentioned as 'OVD' can also be in equivalent e-document, issued by the same issuing authority and with a valid digital signature or the document to the digital locker account of the customer as per the provisions of the Information Technology Act, 2000

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

The OVD and other documents of those Non- Resident Indian (NRI) and Persons of Indian Origin (PIO), whose due diligence is undertaken by the Bank while they are abroad need:

- i. the certification as required under Foreign Exchange Management (Deposit) Regulations, 2016 or
- ii. the verification by the Bank staff from an independent source like passport Seva Kendra, embassy etc. coupled with a video- based liveness verification.

Enhanced due diligence

In case of high-risk customers additional information on the customer beyond documentary evidence of identity and address proof is obtained for opening of the account. This includes

- Information on net worth.

- Intended business activity.
- Report by Relationship Manager/ Branch Manager.
- Higher level approval.
- Verification of customer information with independent data sources wherever publicly available.

High Risk Customers identified at the onboarding stage shall be allowed to open/ operate the account only after completing the EDD to the satisfaction of the Bank. High Risk Customers identified during the periodic risk categorization or transaction monitoring will be followed up for EDD

Third Party due diligence

The Bank relies on customer due diligence done by third parties, for completion of CDD, provided.

- Necessary information/documents of such customers 'due diligence' carried out by the third party is obtained by Bank within two days from the third party or central KYC records registry.
- Adequate steps are taken to satisfy that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be available from the third party upon request within two days or from the Central KYC Records Registry.
- The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act/Rules
- The third party shall not be based in a country or jurisdiction assessed as high risk.

Periodic updation of KYC

The Bank will carry out a system of periodic updation of customer identification data including photograph after complying with full KYC when the account is opened. Fresh proof of identity and address in the case of individuals at the time of periodic updation is not sought in case there is no change in their status with respect to identity and address. A self-declaration by the customer will suffice in such case and can be obtained through customer's registered email id/mobile number, ATMs, other digital channels, or letter. Where the change is only in the address details, a self-declaration of the new address is obtained, and the declared address is verified through positive confirmation within two months by contact point verification of address verification letter/deliverables.

In case of Legal entities, a self- declaration, is obtained if there is no change in the KYC information. Both through Customer declaration and verification of available documents the Bank shall ensure that Beneficial Ownership (BO) information is update. However, if there is a change in KYC information, the process equivalent to fresh on-boarding will be undertaken.

Bank will ensure that the KYC documents on record of the Bank are as per this Policy requirement and valid as on date. If it is not the documents are to be collected afresh as per this Policy requirement and verify the PAN (if available) from the database of the issuing Authority.

Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major. CDD documents of the minor turning to major shall also be ensured to be up to date.

Freezing and Closure of KYC non-compliant account.

Bank shall not open new accounts without PAN or equivalent e-document or Form No.60 (collectively referred as PAN) for clients. For existing clients, the Bank will temporarily freeze the operations in the account, either partly or in full for the failure of the customer to submit the PAN on time. The customer will be intimated at least one month in advance of the possibility of such freeze. However, in case of any urgency the Bank may decide to issue post facto notice of the freeze to the customer. The Bank shall ensure that the Bank's right to apply freeze on KYC grounds has been contractually agreed with the customer in the account opening form and operating terms and conditions.

Walk-in Customer

In case of transactions carried out by a walk-in customer, where the amount of transaction is equal to or exceeds INR. 50,000/- as a single transaction or several transactions that appear to be connected, the customer's identity and address will be verified.

Issue of Demand Drafts, etc. for INR.50, 000.00 and above

Bank will ensure that any remittance of funds by way of demand draft, mail, NEFT/RTGS or any other mode and issue of traveller's cheques for value of INR.50,000/- and above is affected by debit to the customer's account or against cheques and not against cash payment.

Unique Customer Identification Code (UCIC)

The Bank will allot UCIC while entering into new relationships with individual customers and other walk-in customers, who have frequent transactions with the Bank.

The adoption of customer acceptance policy and its implementation will not become too restrictive to result in denial of banking services to general public, specially to those, who are financially or socially disadvantaged. Sufficient flexibility in the requirement of documents of identity and proof of address has been provided in simplified due diligence for accepting a customer to avoid financial exclusion particularly in rural and semi urban areas for opening small accounts to provide basic Banking services to all.

Risk Assessment

The Bank shall carry out Money Laundering and Terrorist Financing 'Risk Assessment 'exercise periodically to identify, assess and take effective measures to mitigate the risk for clients, countries or geographic areas, products, services, transactions, or delivery channels.

Customer profile

The customer profile is a confidential document and the details contained therein will not be divulged for cross selling or for any other purpose and shall be that relevant to the risk category of the customer and not intrusive.

Risk categorization

For the purpose of risk categorization, individuals / entities (other than High Net worth) whose identities and source 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. While considering customer's

identity, the ability to confirm identity documents through online or other services offered by issuing authorities are factored in. The Bank also demarcates certain domestic locations as high risk based on the inputs from AML Monitoring Department where fraudulent transactions were identified.

Terrorist and Unlawful Activities Prevention

The Bank will not open any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

Freezing Assets under Section 51A of Unlawful Activities Prevention Act (UAPA),1967-The procedure laid down in the UAPA Order dated 2nd February 2021 (Annexure 5) of this policy shall be strictly followed and meticulous compliance with the order issued by the Government shall be ensured.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

Special attention shall be given 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 and jurisdictions included in FATF statements and written findings together with all documents shall be retained and shall be made available to Reserve Bank of India/other relevant authorities, on request.

Correspondent Banking

Bank will gather sufficient information to understand fully the nature of the business of the correspondent / respondent Bank. Information on the other Bank's management, major business activities, level of AML / CFT compliance, purpose of opening the account, identity of any third-party entities that will use the correspondent Banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. The correspondent Bank will also ensure that the respondent Bank is able to provide the relevant customer identification data immediately on request.

Correspondent relationship with a 'Shell Bank.'

Shell Banks are not permitted to operate in India. Bank will not enter into relationship with shell Banks and before establishing correspondent relationship with any foreign institution, Bank will take appropriate measures to be satisfied that the foreign respondent institution does not permit its accounts to be used by shell Banks.

Issuance of Prepaid Payment Instruments (PPIs)

Bank will ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India are strictly adhered to in case of issuing PPIs.

Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

- The Bank shall identify all Reporting Financial Institutions under Income Tax (IT) Rule 114F to comply with the provisions of IT Rules 114G and 114H and FATCA and CRS
- Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions.

- Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report.

Bank shall refer to the spot reference rates published by Foreign Exchange Dealers Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H..

Preservation of Records.

Bank will maintain the records (hard and soft copies) containing information in respect of transactions, all necessary records of transaction, which will permit reconstruction of individual transactions .All records of transactions as well as identity and address of customer are required to be maintained and preserved for five years from the date of cessation of the transaction between the client and the Bank.

Sharing KYC information with Central KYC Records Registry (CKYCR)

Bank shall capture the KYC information for sharing with the CKYCR, as required by the applicable KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.

Customer Education / Training of Employees / Hiring of Employees.

It will be ensured that for compliance of KYC norms, customers will be dealt with politely. The front office staff of the branches will educate the customers about relaxed KYC norms, wherever required.. Bank will have constant training programmes so that the member of the staff is adequately trained in KYC procedures. Adequate screening mechanism to ensure strict adherence to the prescribed norms are an integral part of its recruitment/ hiring process of personnel.

SANCTIONS

The Bank shall ensure compliance of sanction requirements, emanated from United Nations, European Union, United States, United Kingdom or any Authority, recognized or legalized in India. In all other cases of international sanctions (not legalized in India) the Bank may reject or refuse to undertake transactions for its constituents or third parties on any actual or perceived financial or regulatory or reputational risk.

Prohibitions

- i. The Bank shall identify the entities and individuals through its CDD process.
- ii. Individuals or entities operating in a Country/ Region under sanction will not be onboarded to the Bank's customer base unless there are specific exemptions in the sanctions for certain types of trade or goods.
- iii. The Bank considers preventive controls such as blocking access to the Sanctioned Countries/Regions Banking digital platform, identifying fax or emails emanating from such countries.
- iv. The Bank adheres to the specific requirements set by the Authorities in respect to entities that have been listed under Sectoral Sanctions, known as Sectoral Sanctions Identifications (SSIs).

Sanctions Screening

Sanctions screening is a control required to be employed by the Bank to detect, prevent and manage sanctions risks and should be undertaken as part of an effective combating of Financial Crimes, to assist with the identification of sanctioned individuals and organisations, as well as the illegal activity to which the Bank can be exposed.

Sanctions screening shall be commensurate with the nature, size and complexity of the risks and must be identified if the same is within the following parameters.

- i. The jurisdictions where the Bank is located and its proximity – geographical, culturally and historically- to sanctioned countries.
- ii. Volume of transactions and distribution channels.
- iii. Nature of business undertaken and place where the customers are located.
- iv. What products and services the Financial Institution/Bank offer and whether those products represent a heightened sanction risk, for example- cross border transactions, foreign correspondent accounts, trade related products or payable through accounts.
- v. Counter parties of our clients (If a Financial Institution is our client, then the client of that Financial Institution) with whom trade/transactions are carried out and the location and business of these counter parties.

Anti-Bribery and Corruption (ABC)

Key Principles

- i. The Bank prohibits its employees and Associated Persons from offering, promising, accepting or requesting any bribe or being involved in any activity or participating in corruption in any form, whether directly or via third parties.
- ii. Prohibits its staff from making or receiving Facilitation Payments, even where this represents local practice or custom. “Facilitation Payment” is a payment which is not officially required or sanctioned but which is made to a Public Official to speed up or otherwise facilitate the performance of duty or function, which the Official is required to perform in any case.
- iii. Prohibits the offering, promising, transferring or acceptance of Anything of Value including gifts, hospitality or entertainment as an inducement to anyone including Public Officials to act improperly so as to obtain or retain business or a business advantage for the group.
- iv. Prohibits making of political donations undertaken by or on behalf of the Bank.
- v. Requires that appropriate risk assessment and /or due diligence must be conducted in respect to Associated Persons, who are Service Providers for the Bank and appropriate contractual terms and governance arrangements must be applied to Associated Persons on a risk – sensitive basis.
- vi. Prohibits the use of employment opportunities- whether permanent or temporary – as an inducement to act improperly to obtain or retain business or business advantage for the Bank, or to influence a Public Official for this purpose. Care must be taken where employment

opportunities are referred by or extended to Public officials, close associates of Public Officials and those closely associated with customers (current or prospective).

- vii. Requires maintenance of books and records of transactions and decisions.
- viii. Will not sanction or otherwise disadvantage any employee or Associated Person for refusing to commit (or assist others in committing) Bribery or Corruption.

WEAPONS OF MASS DESTRUCTION

The weapons of mass destruction used without proper and adequate controls can result in crime against humanity and involving or supporting the sale and purchase of weapons of mass destruction could attract legal, regulatory and reputational issues. The arms deal among Governments, military organisations, agents and middlemen are also susceptible to Financial Crime risk involving money laundering, bribery, corruption and sanction breaches.

Any weapon or mechanism designed to kill, maim or torture humans including Nuclear, Biological or Chemical Weapons, Mines, instruments of torture, weapons or munitions like missiles, rockets, artillery shells and bullets are termed as “weapons of Mass destruction”.

KEY PRINCIPLES

1. The Bank shall frame appropriate process to identify the Defence Companies through the CDD process and may reject the onboarding of such Companies, if the activity is not in the Bank’s risk appetite.
2. Transaction surveillance to identify any deal involving Weapons of Mass destruction by Corporates /individuals not identified as Defence Companies shall be in place.
3. A framework to identify the items notified under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005 during credit approval process shall be established. The Bank shall not facilitate any transaction which is prohibited or regulated under the Act
4. All escalations under the transaction surveillance will be considered for appropriate risk mitigations.