नेपाल एसबिआई बैंक लिमिटेड

NEPAL SBI BANK LTD.

Summary of KYC, AML & CFT Policy

Reviewed on 29th September 2021

Summary of KYC/AML/CFT Policy of Nepal SBI Bank Limited

Background

Asset (Money) Laundering Prevention Act, 2064 (ALPA) and Asset (Money) Laundering Prevention Rules, 2073 (ALPR) formulated by Government of Nepal are in force in the country for the purpose of preventing the country from the risk of asset (money) laundering and terrorist financing. Moreover, Nepal Rastra Bank (NRB) has issued its directives in relation to prevention of asset (money) laundering and combating of financing of terrorist activities to be followed by Banks and Financial Intuitions (BFIs). Financial Information Unit of Nepal (FIU-Nepal), the financial intelligence unit of the country, responsible for receiving, processing, analyzing and disseminating financial information and intelligence on money laundering and terrorist financing activities, also prescribes the guidelines and standards to be followed BFIs.

Being a joint venture partner as well as foreign subsidiary of State Bank of India (SBI), Nepal SBI Bank Ltd. (NSBL) has also taken into cognizance AML/CFT Policy of State Bank of India (SBI) to the extent of applicability.

Therefore, with a view to address and comply with the provisions of ALPA, ALPR, Directives of Nepal Rastra Bank and FIU-Nepal in respect of AML/CFT and to formulate necessary policy, procedural guidelines to combat Assets (Money) Laundering and Combating of Financing of Terrorism, the Bank's Board of Directors has reviewed this Policy and Procedural Guidelines on Know Your Customer (KYC), Anti Money laundering (AML) and Combating of Financing of Terrorism (CFT) of the Bank in line with the stipulations of ALPA, ALPR and Directives of Nepal Rastra Bank and FIU-Nepal.

Policy and Procedural Guidelines on KYC, AML, CFT, hence, encompasses, inter alia, provisions stipulated under recommendations of Financial Action Task Force (FATF), which serve as the international standard for combating of money laundering and financing of terrorism and proliferation of weapons of mass destruction and relevant provisions prescribed by State Bank of India (SBI) through its Policy and Procedural Guidelines on KYC, AML & CFT to the extent of their applicability.

Policy incorporates the following broad key elements:

1. Money Laundering

Money Laundering is a process by which criminal disguises the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. It is the process whereby proceeds of crimes such as drug trafficking, smuggling (alcohol, arms), kidnapping, gambling, robbery, counterfeiting, bogus invoicing, tax evasion, misappropriation of public funds and the like are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds. There are three stages involved in money laundering: placement, layering and integration.

i) Placement

It is the initial stage of money laundering, where "dirty" cash or proceeds of crime from the source enters into the financial system. It is during the placement stage that money launderers are the most vulnerable to being caught.

ii) Layering

The second stage in money laundering is layering. In this stage, money launderers carry out series of conversions or movement of fund mostly to distance from their original source. By way of layering, launderers make it more difficult to detect and uncover a laundering activity.

iii) Integration

The final stage of the money laundering process is termed as integration. It is at the integration stage where the money is returned to the criminal, after series of transactions, from what seem to be legitimate sources.

2. Financing of Terrorism

Financing of terrorism refers to the activities that provide financing or financial support to individual terrorists or terrorist groups or terrorist organizations.

3. Know Your Customer

“Know Your Customer (KYC)” is a process of identifying the customer, verifying their identity, monitoring their transactions, and reviewing their profiles based on risk-based approach and adopting necessary measures to protect the Bank from being the vehicle of money laundering. It is the documented norms for the Bank which enables it to acquire the information pertaining to its customers/clients and the legitimacy of its business/transactions so as to prevent potential risks.

It is the measures implemented to validate the legitimacy of the customers' transactions and their information.

Key elements of the Policy

The key elements of the Policy are as under:

1. **Customer Acceptance Policy**

Bank's Customer Acceptance Policy (CAP) lays down the guidelines for acceptance of potential customers and ensures that only those customers whose identity and purpose of opening accounts or performing transactions can be duly established and verified as legitimate are accepted. Bank shall open account in the name of natural person or any type of entities. The name shall have to be exactly the same and consistent with the one appearing in the identification document. No account shall be opened in the anonymous or fictitious name. Requisite information/documents shall be obtained from the customer for opening account or establishing business relation. No account shall be opened if customer does not provide required information/ document or hides any information or denies providing complete details. Customer cannot be accepted if required information and document is not submitted while initiating any transaction also.

2. **Customer Identification Policy**

Customer identification means undertaking client due diligence measures while establishing business relation e.g., commencing an account-based relationship, but not limited to, including identifying and verifying the customer and the beneficial owners on the basis of the officially valid documents. Customer identification requires identifying the customer and verifying his/her/their identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Policy (CIP) is to be satisfied that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the banking relationship. Customer Identification requirements are different for different types of customers whether they are natural persons or entities. Customer Due Diligence (CDD) is conducted on the basis of information/ documents obtained from customer.

The Bank shall have to identify beneficial owner while establishing business relation with customer or carrying out any transaction. In addition to requirement of identifying beneficial

owners of legal entities, the beneficial owner shall have to be identified even in case of natural persons where beneficial owner other than customer himself/herself exists.

Branches should gather sufficient information to screen its existing as well as potential customer and their beneficial owner to identify the status as Politically Exposed Person (PEP) and/or family members and/or close associates of PEP.

Enhanced Customer Due Diligence (ECDD) is required to be exercised when establishing business relationship or conducting transaction with the customers like- PEP, his/her family member and close associates of PEP, high risk customers, customers conducting complex, unusual large transactions and unusual patterns of transactions or which have no apparent economic or visible lawful purpose, etc. While conducting Enhanced Customer Due Diligence of customer, it should be taken care that the customer should by no means understand such suspect.

Customer Due Diligence is done for all customers. However, there are some circumstances where risk of money laundering or terrorist financing is lower, where information on the identity of customer is publicly available. In such circumstances, Simplified Customer Due Diligence (SCDD) can be applied after identifying and verifying identity of customer and beneficial owners.

3. Risk Categorization

For proper risk assessment of business relationship with customers and evolving suitable monitoring mechanism, all new customers are to be risk-categorized. as High risk, Medium risk, Low risk and Lowest Risk. Based on risk category, high risk customers pose highest level of ML/TF risk whereas lowest risk customers pose nominal level of ML/TF risk. It is to be specifically noted that risk categorization is meant for proper monitoring of customer activity/ transaction and does not reflect in any way on the account holders. Risk Categorizations done by the Branch should not be disclosed to the customers.

Branch should ensure that risk categorization of all customer accounts is completed and thereafter reviewed at least in the following frequency.

- For high-risk customers- At least once a year
- For medium risk customers- At least once in every three years
- For low-risk customers- At least once in every five years
- For lowest risk customer (In case of low-risk customer whom Simplified Customer Due Diligence is applicable)- At least once in every eight years

4. Monitoring of transactions

Monitoring is an ongoing and essential element of KYC, AML and CFT. Bank shall exercise the ongoing monitoring and due diligence to ensure that account/ transactions are used for legitimate purpose and by no means are used in Money Laundering or Terrorist Financing or any other illegitimate activities. Transactions should also be monitored depending on the risk sensitivity of customer. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no lawful purpose.

5. Miscellaneous

- Reporting requirements

  In terms of ALPA and NRB Directives, AML Compliance Officer is obliged to file various reports to the Financial Information Unit-Nepal (FIU-Nepal) which has been set up as a national unit, for interalia, collecting, analyzing, and disseminating information in respect of financial transactions. Threshold Transaction Report (TTR), Suspicious Transaction Report (STR) and other reports as sought is to be submitted to FIU. Similarly, reports as per regulatory requirement is also to be submitted to Nepal Rastra Bank.

- Maintenance and Preservation of Records

  All information, details, documents, reports, conclusion of analysis and records shall have to be mentioned accurately and securely for minimum 10 years after termination of business relation with the customer or from the date of transaction or from the date of occasional transaction. All information, documents and records shall have to be maintained in such a way that each transaction is clearly visible and the same is sufficient to be produced as evidence in the course of legal proceedings. Records shall have to be maintained in readily available form for submission to competent authority on demand.

- Combating of Financing of Terrorism

  As per the provision of ALPA, as and when list of terrorist individuals, group or organizations are received for freezing their fund or assets, as approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), Ministry of Foreign Affairs may publish such updated list of listed individual, group or organization in its website and it further sends the same promptly to Ministry of Home Affairs through Electronic channel. Accordingly, Ministry of home Affairs publishes such updated list of terrorists along with freeze

order in its website at https://www.un.org/securitycouncil/content/un-sc-consolidated-list. In addition, Ministry of Home Affairs shall also publish the list of individual, group or organizations found to be involved in terrorist activity as per the decision of government of Nepal based on the investigation of Ministry of Home Affairs as per its own findings or request received from foreign countries through Ministry of Foreign Affairs of Nepal at its website with freeze order. Banks should ensure to update the consolidated list of such terrorist individual, group or organization by regularly visiting the website of Ministry of Home Affairs and should immediately freeze the fund or assets of such terrorist individual, group or organization.

Moreover, in terms of Section 110 of the Banks and Financial Institutions Act, 2073, Nepal Rastra Bank may direct banks to freeze any account opened in the concerned licensed institution in the name of any individual, firm, company or institution in such a manner as to prevent the withdrawal or transfer of funds in any way from that account in connection with investigations into any type of crime or in connection with protecting the national interests by checking money laundering and terrorist activities or organized crimes.

- Correspondent Banking

  Transactions conducted through correspondent banking relationships need to be managed taking a risk-based approach. "Know Your Correspondent" procedures should be established to ascertain whether the Correspondent Bank or counter-party is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of their customers as per Financial Action Task Force (FATF) standards. Due diligence measures need to be applied while establishing correspondent banking relation and carrying out transaction with them. No correspondent banking relation is to be established with shell banks.

- Wire Transfers

  Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. There is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. Required minimum information is to be obtained for accurate identification and verification of customer irrespective of the currency and amount.

- Relationship with vendors, service providers and other parties

  The Bank shall have to obtain relevant information/documents as deemed necessary and carry our initial due diligence while establishing relationship with vendors, service providers and other parties such as business partners, consultants, valuators, etc. All functionaries in the Bank will ensure at the time of approving outsourcing services that KYC/AML/CFT measures are implemented in letter and spirit and no access is given to any individual/entity having direct/indirect link to banned entities/individuals.

- Downward Correspondent Banking

  The Bank shall not provide/permit downward correspondent banking service and nested account activities to other financial institutions unless concerned correspondent bank permits/ provides consent for the same.

- Payable Through Accounts

  The Bank will not provide customers with the services of payable through accounts i.e., direct access to any of its correspondent account held with foreign banks.

- Introduction of New Technology

  Bank will pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent its misuse for money laundering activities. Bank will ensure that appropriate KYC procedures are duly applied to the customers using new technology driven products. Moreover, the bank shall assess the AML/CFT risk and arrange for necessary procedure/mechanism for managing the same while introducing any new technology, product or service.

- Resubmission Policy

  Once the transaction is rejected by Bank due to sanctions/ money laundering/ terrorist financing concerns, concerned department/ branch shall maintain record of such rejected transactions and shall not accept the same submitted by correspondent bank after stripping off information. Moreover, the Bank shall maintain record of transactions rejected by correspondent bank and shall not attempt to resubmit same transaction after stripping off information.

- Importance of KYC for Employees

  KYC of employees is conducted in accordance with the highest ethical standards and the extant regulatory requirements and laws. Staff should not provide advice or other assistance to individuals who are indulging in money laundering activities. KYC norms/ AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse channels of the Bank. Bank will put in place necessary and adequate screening mechanism as an integral part of its recruitment/hiring process of personnel. Ongoing employee training programs should be conducted so that staff members are adequately trained in KYC/AML/CFT policy and procedures.

- Tipping Off & Confidentiality

  The Bank and branches/ extension counters/departments shall maintain the details of all transactions of unusual/ suspicious activity reported, STRs, TTRs and correspondence record to and from FIU, NRB and other investigating authorities relating to its customers/transaction under the investigation strictly confidential and will not share the same with the customer or any irrelevant bank staffs, unrelated official meetings or anyone outside the bank. Doing so would constitute “Tipping Off”, which is an offense prohibited by law. The bank is required to keep the documents, information and transaction details of the customer confidential and will not leak/share to unauthorized person.

- Capacity enhancement programs for Board Members & Top Management

  For effective and result-oriented implementation of AML/CFT provisions as per ALPA, ALPR and NRB Directives, the bank shall arrange knowledge sharing programs on AML/CFT for capacity enhancement of Board members, top management and shareholders having 2% or more share of paid-up capital at least once a year and at more frequent intervals upon requirement.