

Sudanese French Bank

POLICY FOR PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

INTRODUCTION:-

The policy of Sudanese French Bank, is based on management of compliance risks arising from customers; and it also oversees: Ongoing compliance with the requirements introduced by the national and international laws, regulations and sanctions, Implementation of the risk-based “Know Your Customer” and “Customer Activity Monitoring” principles, determination and reporting of the suspicious transactions, preservation of reputation and brand value of the Bank towards national and international authorities. Laundering of proceeds of crime and financing of terrorism may arise diversely from various fields of activity. Risk-based approach enables the measurement of risks for potential laundering of proceeds of crime based on the field of activity, identification of the criteria, and activation of the appropriate means and methods for mitigating and controlling such risks. For the purpose of preventing any transactions with respect to laundering of proceeds of crime and financing of terrorism, SUDANESE FRENCH BANK, arranges and organizes the works required for implementation of adequate procedures in relation to monitoring the customers’ transactions, related reporting, retention of records, and organization of the training activities and performance of the internal auditing activities, with a risk-based approach; and ensures that any risks falling under such scope are controlled.

RISK MANAGEMENT ACTIVITIES:-

The primary purpose of the risk management policy is to ensure identification, assessment and scoring of risks, action planning and

mitigation of the potential risks the Bank may be exposed to, in relation to laundering of proceeds of crime and financing of terrorism. To that end, the Bank has developed “Know Your Customer” and “Customer Activity Monitoring” risk assessment principles

Know Your Customer:-

As per article 3 of the Law numbered (2014), the obliged parties shall identify the persons carrying out transactions and the persons on behalf or account of whom the transactions are conducted within or through the obliged parties before the transactions are conducted. To that end, “Principles regarding customer due diligence” are set out under chapter three of the “Regulation on the Measures Regarding Prevention of Laundering of Proceeds of Crime and Financing of Terrorism”. Accordingly, the bank performs necessary controls and takes additional measures with respect to:

- Identification and verification of the valid identity and address details of (potential) customers, acceptable to the legal authorities, before performing a transaction and during the course of a continuous business relation;
- Consistency of the income levels of customers and the financial services they perform/request with their business, the general course of action and sources of income of the customer type, in which they are included;
- Possibility of the customers being included on national/international sanctions lists.

The Bank does not establish any business relations or perform the transaction requested if the proof of identification and verification is not made or sufficient information about the purpose of the business relations is not obtained; and the business relation will be terminated, when the identification and verification of the customer is not performed where it is required to be conducted in case of any suspicion related to sufficiency and accuracy/authenticity of the previously obtained identity details of the customer.

The standard customer due diligence process to be performed by the Bank, at a minimum, as part of “Know Your Customer” measures includes:

- Identification and verification/authentication of the customer’s identity details, address, specimen signature, ultimate beneficial owners, authorized representatives in accordance with legal legislation and the internal policies of Sudanese French Bank.
- Screening of the customers in case of the risk of them being on international sanctions lists (including country risk assessment).
- Determination of whether the customer and any related parties of the customer are a politically exposed person (PEP), or related/linked to a politically exposed person, Investigation of whether the customer and related parties of the customer are associated with ultra high risk countries as defined under international sanctions and Internal Policies.
- Determination of whether the customer acts on behalf and/or account of other persons.
- Monitoring of customer transactions for detection of any unusual transactions.
- Identification and verification of the source of income.
- Obtaining information about the reasons for working with the bank.

In addition, enhanced due diligence measures are applied for customers who are regarded as risky by the Bank as a result of the risk assessment to be performed during customer acceptance processes or subsequently. Notwithstanding the results of the risk assessment, application of enhanced measures and/or update of monitoring operations may be considered in accordance with the risky customer/transaction/sector assessments under national and international regulations and applicable banking practices.

The measures to be taken by the Bank as part of the enhanced customer due diligence process include:

- Identification of the customer, beneficial owner, authorized representatives (including composition of the company) and filtering of the same in case there is a risk of them being in international sanctions lists.
- Related business line/senior management approval for customer relationship,
- Identification and verification, where necessary, of source of wealth of the customer and the ultimate beneficial owner based on documentation.
- Determination of whether the source of funds and/or capital of the customer have been verified in an easy and satisfactory manner and authentication of the same based on documentation, where necessary.
- Control of the information and the documentation regarding the reasons of working with the Bank.

Risk Assessment Methodology:-

All customers should undergo an assessment process in respect of potential risks of laundering of proceeds of crime and the associated risks as part of the minimum standards set out under Regulatory Controls of the Central Bank of Sudan (No.8/2014). For this purpose, the Bank implements a customer risk assessment methodology which takes into account:

- The geographical location where the customer operates (country, region, etc.).
- Certain products and services provided to the customer.
- Whether the customer is a politically exposed person or not.

- The line of business of the customer or the industry in which the customer operates.
- The type of transactions performed by the customer.
- The shareholding structure, capital and senior management, controls of the customer.

This methodology is revised by the Bank when a new risk specific to a customer or certain transactions arises, and the Bank takes necessary measures in this respect.

The Bank should identify and verify account numbers, ultimate beneficial owners, authorized representatives and shareholding/control structure of the customers; and perform the detailed investigation measures of the customers in accordance with the general requirements prescribed under the regulations.

As part of the risk assessment methodology, the persons and entities, for whom/which the Bank shall not intermediate any financial transactions or which shall be subjected to enhanced measures in establishment of the business relation are listed below:

- Any persons and entities refraining from; providing information, documentation and being subject to recording,
- Any persons or entities present in national and international sanctions lists.
- Any persons or entities involved in risky sectors and occupational groups.
- Any persons or entities located in or associated with countries without satisfactory regulations in place with respect to prevention of laundering of proceeds of crime and financing of terrorism (risky countries).
- Shell banks.
- Politically exposed persons (PEPS).

MONITORING AND CONTROL ACTIVITIES:-

For the purposes of prevention of laundering of proceeds of crime and financing of terrorism, the Bank carries out a monitoring and control process, at a minimum, in relation to:

- High-risk customers and transactions.
- Transactions with the risky countries.
- Complex and unusual transactions.
- Transactions inconsistent with the customer's business.
- Source of funds and profile.
- Associated transactions.
- Electronic transfers.
- Non-face-to-face transactions.
- Newly introduced products and services.

Accordingly, the Bank carries out the following activities for monitoring of the services provided and transactions intermediated by the Bank.

REPORTING OF SUSPICIOUS TRANSACTIONS:

Suspicious transaction means presence of any information, or any matter which would require suspicion about the fact that the assets subject to a transaction, performed or attempted to be performed with or through the agency of the Bank, have been obtained illegally, or are used for unlawful purposes, or are used by any terrorist organizations, terrorists or financiers of terrorism within such scope, or are related or associated with them.

Definition of the term "Suspicious Transaction" includes use of the assets, subject to the transaction, for unlawful purposes in addition to the fact that they have been obtained illegally; and it shall purport to include prevention of financing of terrorism (even if such assets are not associated with financing of terrorism) thereby.

The Bank shall not provide any information to any person, including the persons who are a party to the relevant transaction, other than the information provided to the supervisory staff members commissioned with the duty of supervision of the obligation, as well as to the courts during the course of any trial, that a suspicious transaction reporting has been sent or will be sent to the (Financial Information Unit). Such obligation shall also apply with respect to the persons, entities, organizations, who/which have reported the suspicious transaction to the (FIU) and also their members who/which have actually performed or managed such transaction, or the legal representatives and agents of the same, and also any other staff member who is in any way acquainted with the fact that a suspicious transaction has been reported.

PROVISION AND RETENTION OF INFORMATION AND DOCUMENTATION:

The Bank implements the processes with respect to provision of information and documentation as per (2014 Sudanese Anti Money Laundering act) and “Regulation from Central Bank of Sudan NO 8/2014) on the Measures Regarding Prevention of Laundering of Proceeds of Crime and Financing of Terrorism”, and takes necessary actions and measures accordingly.

The Bank retains any documents associated with its obligations (including training and internal audit report), and for a period of five years to start as of the date of issuance, and for a period of five years as of the date of the last entries/records for the books and, and as of the date of the last transaction for the documents and entries/records regarding due diligence; and it presents any such documents and entries/records to the officials upon request.

TRAINING ACTIVITIES:

Training activities are planned according to the Bank's internal programs, and training in a manner that covers:

- Particulars about the internal compliance officer of the Bank, and the channels for reporting the suspicious transactions,
- The concepts of laundering of proceeds of crime and financing of terrorism,
- Risk areas,
- Principles with respect to customer due diligence.
- Suspicious transaction reporting.
- Suspicious transaction types.
- Obligation to provide information and documents, sanctions to be applied in case of any failure to observe and fulfill the obligations,
- International regulations with respect to prevention of money laundering and financing of terrorism.

INTERNAL AUDIT ACTIVITIES:

The INTERNAL AUDIT examines and inspects, annually and with a risk-based approach, whether the internal policies and procedures, risk management, monitoring and control activities and the training activities are adequate and effective or not, whether the risk policy is adequate and effective or not, and whether the procedures and transactions are being performed in accordance with the Law and the regulations.