Alpha Alternatives Financial Services Pvt Ltd

Know Your Customer & Anti-Money Laundering Policy

Version 3.0
Date: 15th May, 2023
Last Reviewed Date: 21st April, 2025

Table of Contents

1. Introduction

(i) RBI has issued directions called the Reserve Bank of India (Know Your Customer) Directions, 2016, as amended from time to time, the latest being vide RBI Master Direction DBR. AML. BC.No.81/14.01.001/2015-16 dated February 25, 2016 (updated as on November 06, 2024) on Know Your Customer (KYC), to all the Regulated Entities (REs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti-Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) Policies.

(ii) In terms of para 4 of the RBI Master Direction on KYC, the KYC Policy is duly approved by the Board.

2. Group-wide Policies

(i) In terms of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-Laundering Act, 2002 (PML Act).

(ii) The NBFC, which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(iii) The Group shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961

3. Definitions

Unless the context is otherwise required, the terms herein shall bear the meanings assigned in terms of the PML Act, 2002 and PML Rules, 2005.

(i) Beneficial Owner

(a) If the customer is a company: The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation:

“Controlling ownership interest” means ownership of/entitlement to more than 10% of the shares or capital or profits of the company. “Control” means the right to appoint

majority of directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

(b) If the customer is a partnership firm: The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10% of capital or profits of the partnership or who exercises control through other means.

(c) If the customer is an unincorporated association or body of individuals: The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15% of the property or capital or profits of the unincorporated association or body of individuals.

Explanation:

The term “body of individuals” includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(d) If the customer is a trust: The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

(ii) Central KYC Records Registry (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. Every RE within 10 days after the commencement of account- based relationship with the customer, shall file the electronic copy of the customer’s KYC records with CKYCR.

Whenever the RE obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the RE shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC

record of an existing customer, the RE shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the RE.

For the updation/ periodic updation or for verification of identity of a customer, the RE shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless:

(a) there is a change in the information of the customer as existing in the records of CKYCR, or

(b) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms, or

(c) the validity period of downloaded documents has lapsed, or

(d) the RE considers it necessary to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

(iii) Customer means a person who is engaged in a financial transaction or activity with an RE and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

(iv) Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. The data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by RBI. The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding Rs.50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose, and intended nature of the business relationship, where applicable.

(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control.

(c) Determining whether a customer is acting on behalf of a beneficial owner and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

(v) Digital KYC means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the PML Act.

(vi) Digital Signature shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

(vii) Equivalent e-document means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016

(viii) Know Your Client (KYC) Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry.

(ix) Money Laundering

Section 3 of the Prevention of Money Laundering Act (PMLA) defines money laundering as whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering. The proceeds of crime mean any property derived or obtained, directly or indirectly, by any person because of criminal activity relating to a scheduled offence or the value of any such property.

(x) Officially Valid Document (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, provided that:

(a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

(b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address: utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill, etc.), property or municipal tax receipt, pension or family pension payment orders (PPOs) issued to retired employees by government departments or public sector undertakings, if they contain the address, letter of allotment of accommodation from employer issued by state government or central government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

(c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at (b) above

(d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents 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.

Explanation:

A document shall be deemed to be an OVD even if there is a change in the name after its issuance provided it is supported by a marriage certificate issued by the state government or gazette notification, indicating such a change of name.

(xi) On-going Due Diligence means regular monitoring of transactions in accounts to ensure that those are consistent with NBFC's knowledge about the customers, customers' business and risk profile, the source of funds/wealth.

(xii) Person, as defined in the PMLA includes:

(a) an individual,

(b) a Hindu undivided family,

(c) a company,

(d) a firm,

(e) an association of persons or a body of individuals, whether incorporated or not,

(f) any artificial juridical person, not falling within any one of the above (a) to (e), and

(g) any agency, office/branch owned/controlled by any of the above (a) to (f).

(xv) Regulated Entities (REs) means

(a) all the banks, viz., scheduled commercial banks (SCBs)/ regional rural banks (RRBs)/ local area banks (LABs)/ primary (urban) co-operative banks (UCBs)/state and central co-operative banks (StCBs/CCBs) and any other entity which has been licensed under Section 22 of the Banking Regulation Act, 1949

(b) All India Financial Institutions (AIFIs)

(c) All Non-Banking Finance Companies (NBFCs)

(d) Asset Reconstruction Companies (NBFCs)

(e) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

(f) All authorised persons (APs), including those who are agents of Money Transfer Service Scheme (MTSS)

(xiii) Suspicious transaction means a transaction as defined below, including an attempted transaction, whether made in cash, which, to a person acting in good faith:

(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the schedule to the Act, regardless of the value involved; or

(b) appears to be made in circumstances of unusual or unjustified complexity; or

(c) appears to not have economic rationale or *bona-fide* purpose; or

(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation:

A transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

(xiv) Video based Customer Identification Process (V-CIP)

V-CIP is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP.

4. Objective of the policy

(i) to ensure compliance with PML Act, and PML Rules, including regulatory guidelines in this regard

(ii) to provide a bulwark against threats arising from money laundering, terrorist financing, etc. by adoption of best international practices like the Financial Action Task Force (FATF) Standards and FATF Guidance Notes.

5. Key elements of the policy

(i) Customer Acceptance Policy

(ii) Risk Management

(iii) Customer Identification Procedures, and

(iv) Monitoring of Transactions

6. Money Laundering and Terrorist Financing Risk Assessments

The NBFC to carry out 'Money Laundering and Terrorist Financing Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

7. Role of the Designated Director

(i) The designated director means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules and shall include:

(a) the MD/WTD, duly authorised by the Board, if the RE is a company,

(b) the managing partner, if the RE is a partnership firm,

(c) the proprietor, if the RE is a proprietorship concern,

(d) the managing trustee, if the RE is a trust,

(e) a person or individual who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

(f) a person who holds the position of senior management or equivalent designated as a director in case of co-operative banks and regional rural banks.

(ii) The MD/CEO is the designated director, as nominated by the Board.

(iii) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

(iv) The name, designation, address, and contact details of the Designated Director shall also be communicated to the RBI.

8. Role of the Principal Officer

(i) The principal officer means an officer at the management level nominated by the NBFC, responsible for furnishing information under Rule 8 of the PML Rules.

(ii) The Chief Finance Officer (CFO), as the key managerial personnel, or in absence of the CFO, the Head of Accounts Section is responsible for furnishing the requisite information under the PML Rules.

(iii) The principal officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

(iv) The name, designation and address of the principal officer shall be communicated to the FIU-IND.

(v) The name, designation, address, and contact details of the principal officer shall also be communicated to the RBI.

9. Customer Acceptance Policy

(i) The NBFC shall file a suspicious transactions report (STR), if necessary, when it is unable to comply with the relevant CDD measures in relation to a customer, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

(ii) The NBFC shall not undertake any transaction without following the CDD procedure.

(iii) The circumstances in which, a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out, and documented.

(iv) The NBFC shall ensure that the identity of the customer does not match with any person or entity, whose name appears in the Sanctions lists (Annex-1).

(v) The NBFC shall leverage latest technological innovations and tools for effective implementation of name screening to meet the Sanctions requirements.

(vi) Where PAN is obtained, the same shall be verified from the verification facility of the issuing authority. Where an equivalent e-document is obtained from the customer, the digital signature shall be verified, as per the provisions of the Information Technology Act, 2000.

(vii) Where GST details are available, the GST no. shall be verified from the search/verification facility of the issuing authority.

(viii) Where the NBFC forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

(ix) The NBFC shall apply the CDD procedure at UCIC level. Thus, if an existing KYC compliant customer desires to avail any other product or service from the NBFC, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

10. Customer Identification Procedures (CIP)

10.1. The NBFC shall undertake identification of customers in the following cases:

(i) Carrying out any international money transfer operations with a customer

(ii) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

(iii) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs.50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.

(iv) When the NBFC has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/-.

10.2. For verifying the identity of customers, the NBFC may rely on CDD done by a third party, subject to the following conditions:

(i) The records or the information of the CDD carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry (CKYCR), using a KYC identifier.

(ii) The copies of identification data and other relevant documentation relating to the CDD requirements shall be made available by the third party, upon request without delay.

(iii) The third party is regulated, supervised, or monitored for, and has measures in place for, compliance with CDD and record-keeping requirements in line with the requirements and obligations under the PML Act.

(iv) The third party shall not be based in a country or jurisdiction assessed as high risk.

(v) The ultimate responsibility for CDD and undertaking enhanced due diligence measures, as applicable, will be with the NBFC.

11. Customer Due Diligence (CDD) Process

The NBFC shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, and the source of funds/wealth. Without prejudice to the generality of factors that call for close monitoring, the following types of transactions shall necessarily be monitored:

(i) The relevant transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

(ii) All the transactions which exceed the cash transactions of Rs.50,000/- and above and account transactions of Rs.10.00 lakh and above.

12. Risk Assessment of Customers

(i) The NBFC shall adopt a risk-based approach for updation/periodic updation of KYC, ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. The KYC updation shall be undertaken once in a year, two years and five years for the customers in "high", "medium" and "low" categories respectively. The status of the KYC updation of the customers shall be put up to the senior management and shall be placed before the RMC/Board on a half-yearly basis.

(ii) The exercise for risk assessment, and categorisation of accounts shall be carried out at least once in six months and placed before the RMC/Board.

(iii) The risk categorisation shall be undertaken based on the:

(a) customer's profile: viz., customer's identity, social/financial status, nature of business activity, customer's business, source of income, residential status, geographical location, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

(b) customer's financial: viz., legal structure, transparency in ownership, identification of beneficial ownership, business turnover, credit ratings, etc.

(c) credit flagging: types of business operation, types of products/services offered, types of delivery channel used for delivery of products/services, types of transaction undertaken in cash/cheque/monetary instruments/wire transfers/forex transactions, non-face-to face customers, politically exposed persons, etc.

Explanation: Politically Exposed Persons are the individuals who are or have been

entrusted with prominent public functions by a foreign country, including the heads of states/governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations, and important political party officials.

(iv) Broadly, the risk-categorization of customers is as follows:

(a) Low-risk customers: Primary dealers, and FIs regulated by RBI, government departments and government undertakings, insurance companies regulated by IRDA, mutual funds, and portfolio management services regulated by SEBI, listed entities regulated by SEBI, trusts of provident funds, pension funds, gratuity funds, and other superannuation funds recognized by the income tax department.

(b) Medium-risk customers: All individual borrowers in retail portfolio, the customers not falling in high/ low risk categories.

(c) High-risk customers: Politically exposed persons, multi-level marketing companies, dealers in arms/ammunition, dealers in precious metals like gem & jewellery, real estate, auction houses, wilful defaulters, companies prohibited by SEBI from trading in securities, etc.

(v) FATF statement/standard, the reports and guidance notes on KYC/AML issued by the Indian Banks Association, and other agencies, etc., may also be used in risk assessment.

(vi) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

13. Maintenance, and Preservation of Record

Under the provisions of the PML Act and PML Rules regarding maintenance, preservation, and reporting of customer information, the NBFC shall:

(i) maintain all necessary records of transactions between the NBFC and its customer, both domestic and international, for at least five years from the date of transaction.

(ii) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during business relationship, for at least 5 years after the business relationship is ended.

(iii) make available swiftly, the identification records and transaction data to the competent authorities upon request

(iv) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules)

(v) maintain all necessary information in respect of transactions prescribed under PML Rule 3, to permit reconstruction of individual transaction, including the following:

(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.

(vi) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities

(vii) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation:

The expressions “records” pertaining to the identification, identification records, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

(viii) ensure that the details of the customers are registered on the DARPAN Portal of NITI Aayog, in case of customers who are non-profit organisations. If the same are not registered, the NBFC shall register the details on the DARPAN Portal and shall also maintain such registration records for a period of five years after the business relationship between the customer and the NBFC has ended or the account has been closed, whichever is later.

(ix) The NBFC shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the NBFC and its customer. While considering the requests for data/information from government and other agencies, the NBFC shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions. The exceptions to the said rule shall be as under:

(a) where disclosure is under compulsion of law,

(b) where there is a duty to the public to disclose,

(c) the interest of the NBFC requires disclosure, or

(d) where the disclosure is made with the express or implied consent of the customer.

14. Reporting to Financial Intelligence Unit-India (FIU-IND)

(i) The principal officer of the NBFC shall furnish to the director, FIU-IND the information referred to in Rule 3 of the PML Rules in terms of Rule 7 thereof.

(ii) While furnishing information to the director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the PML Rules shall be constituted as a separate violation.

(iii) The NBFC, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in Rule 3 of the PML Rules and furnishing of the information to the director is confidential. However, such confidentiality requirement shall not inhibit sharing of information, for any analysis of transactions and activities which appear unusual, if any such analysis has been done.

(iv) The NBFC shall make use of the editable electronic utilities to file electronic cash transaction reports (CTR)/suspicious transaction reports (STR) placed on its website http://fiuindia.gov.in by FIU-IND.

(v) The NBFC shall install suitable technological tools for extracting CTR/STR from its live transaction data, after fully automation of its operations.

(vi) A robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions

15. Compliance with the KYC & AML Policy

The NBFC shall ensure compliance with KYC & AML Policy through:

(i) the designated director and principal officer, as defined at para 7 and 8 above, for effective implementation of policies and procedures.

(ii) independent evaluation of the compliance functions of the KYC & AML policies and procedures, including legal and regulatory requirements.

(iii) verification of the compliance with KYC & AML policies and procedures by the internal audit, and

(iv) submission of quarterly audit notes and compliance to the ACB.

16. Review of KYC & AML Policy

The Board shall review the KYC & AML Policy on an annual basis, or more frequently, keeping in view the changes in regulations.

Annexure-1: Obligations under International Agreements

1. Obligations under the Unlawful Activities (Prevention) Act, 1967 (UAPA)

(i) The NBFC shall ensure that in terms of section 51A of the UAPA and amendments thereto, it doesn't have 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). The details of the two lists (given at Annexure-2) are as under:

(a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", established and maintained pursuant to Security Council Resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

(b) The "Taliban Sanctions List" established and maintained pursuant to Security Council Resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://www.un.org/securitycouncil/sanctions/1988/materials

(ii) The NBFC shall verify on daily basis lists in the first schedule and the fourth schedule of UAPA, 1967 and the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, for compliance with the government orders on implementation of section 51A of the UAPA and section 12A of the WMD Act.

(iii) The details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA), as required under UAPA notification dated February 2, 2021. The list of Nodal Officers for UAPA is available on the website of MHA.

(iv) The NBFC shall undertake countermeasures, when called upon to do so by any international or inter-governmental organisation, of which India is a member and accepted by the central government.

2. Obligations under Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act)

(i) The NBFC shall ensure compliance with the procedure for implementation of section 12A of the WMD Act laid down in terms of section 12A of the WMD Act vide order dated September 1, 2023, by the Ministry of Finance, Government of India.

(ii) In accordance with paragraph 3 of the order, the NBFC shall ensure not to carry out transactions in case the particulars of the individual/entity match with the particulars in the designated list.

(iii) The NBFC shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc.

(iv) In case of match in the above cases, the NBFC shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved, to the Central Nodal Officer (CNO), designated as the authority to exercise powers under section 12A of the WMD Act. A copy of the communication shall be sent to State Nodal Officer (SNO), where the account/transaction is held and to the RBI. It may be noted that in terms of paragraph 1 of the order, the director, FIU- India has been designated as the CNO.

(v) The NBFC shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(vi) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of section 12A of the WMD Act, the NBFC shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, fax and by post, without delay.

3. UNSCR 1718 Sanctions List of Designated Individuals and Entities

The NBFC shall verify on a daily basis, the UNSCR 1718 Sanctions List of Designated Individuals and Entities, as available at:

https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm,

and consider any modifications to the list in terms of additions, deletions or other changes and ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the central government.

4. Jurisdictions that do not or insufficiently apply the FATF Recommendations

(i) The NBFC shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries, for which this is called for by the FATF. The FATF statements circulated by RBI from time to time, and publicly

available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF statements, shall be taken into consideration for this purpose.

(ii) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to RBI and other relevant authorities, on request.

Annexure-2: UNSC Sanctions

The Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter. The Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force. Since 1966, the Security Council has established 31 Sanctions regimes, in Southern Rhodesia, South Africa, the former Yugoslavia (2), Haiti (2), Angola, Liberia (3), Eritrea/Ethiopia, Rwanda, Sierra Leone, Côte d'Ivoire, Iran, Somalia/Eritrea, ISIL (Da'esh) and Al-Qaida, Iraq (2), Democratic Republic of the Cong, Sudan, Lebanon, Democratic People's Republic of Korea, Libya (2), Taliban, Guinea-Bissau, Central African Republic, Yemen, South Sudan, and Mali.

The Security Council Sanctions have taken different forms, in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied Sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights, and promote non-proliferation.

The Sanctions do not operate, succeed, or fail in a vacuum. The measures are most effective at maintaining or restoring international peace and security when applied as part of a comprehensive strategy encompassing peacekeeping, peace-building and peace-making. Contrary to the assumption that Sanctions are punitive, many regimes are designed to support governments and regions working towards peaceful transition. The Libyan and Guinea-Bissau Sanctions regimes all exemplify this approach.

Presently, there are 15 ongoing Sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counterterrorism. Each regime is administered by a Sanctions Committee chaired by a non-permanent member of the Security Council. There are 11 monitoring groups, teams and panels that support the work of 12 of the 15 Sanctions Committees. In the 2005 World Summit declaration, the General Assembly called on the Security Council, with the support of the Secretary-General, to ensure that fair and clear procedures are in place for the imposition and lifting of Sanctions measures. The establishment of a focal point for de-listing, and the Office of the Ombudsperson to the ISIL (Da'esh), Al-Qaida, & Taliban Sanctions Committee are examples of this approach in practice.