

Pension Funds

Aditya Birla Sun Life Pension Management Ltd.



**ADITYA BIRLA
CAPITAL**

PROTECTING INVESTING FINANCING ADVISING

ADITYA BIRLA SUN LIFE PENSION MANAGEMENT LTD

POLICY ON ANTI MONEY LAUNDERING

Version: 1.2

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 2 of 20	
Document Title: Anti Money Laundering Policy					

Document Version Control

Version	Owner of the Document	Date of Approval by RMC	Date of Approval by Board	Revised Policy Effective from	Nature of Change
1.0	Compliance	27/07/2016	27/07/2016	27/07/2016	New Policy
1.1	Compliance	23/04/2019	23/04/2019	23/04/2019	Updated with applicable regulatory changes, customer due diligence practices and formatting change
1.2	Compliance	20/04/2023	20/04/2023	20/04/2023	Update as per guidelines on Know Your Customer / Anti-Money Laundering / Combating the Financing of Terrorism (KYC / AML / CFT)

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 3 of 20	
Document Title: Anti Money Laundering Policy					

Table of Contents

Sr. No.	Particulars	Page No
I	Introduction	4
I.1	Stages of Money Laundering	4
I.2	Money Laundering in India	4
I.3	Regulatory Framework	5
I.4	AML Program	5
II.1	Internal Policies, Procedures and Controls	5
A	Know Your Customer (KYC) & Customer Identification	5
B	Monitoring of cash Transactions	5
C	Suspicious Transactions	6
D	Monitoring of Suspicious Transactions	6
II.2	Designated Director & Principal Compliance Officer	6
II.3	Record Keeping	7
II.4	Anti Money Laundering Training	7
II.5	Internal Audit and Control	7
II.6	Officially Valid Documents	8
	Annexure A – List of KYC Documents	9

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 4 of 20	
Document Title: Anti Money Laundering Policy					

I. INTRODUCTION

Terrorists' attacks have made the subject of money laundering much more relevant to the stability of modern world. Criminals including terrorists use techniques and tools of money laundering to sustain and finance their operations. Today money laundering is global problem. Magnitude of this problem can be judged from the report of International Monetary Fund (IMF), which states that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's Gross Domestic Product (GDP).

I.1. Stages of Money Laundering

Money Laundering means "any act or attempted act to disguise the source of money or assets derived from criminal activity". The purpose of Money Laundering is to turn 'dirty money' into 'clean money' through a series of financial transactions so that criminal origins of the funds becomes difficult to trace.

Money can be obtained illegally from various criminal activities like drug trafficking, terrorism, organized crime and fraud. As criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities and provide a legitimate cover for their source of income they usually follow three stages:

"Placement": means placing currency into the financial system so as to convert illicit funds from cash straight into a financial instrument or a bank account.

For Example, A criminal having huge crime proceeds in form of cash, can deposit this cash in bank accounts maintained with different banks, in the name of his relatives, friends and associates, in small amounts. Alternatively, he can also invest in insurance policies by paying premium in cash.

"Layering": Now having successfully placed money into the financial system, the second stage is layering.

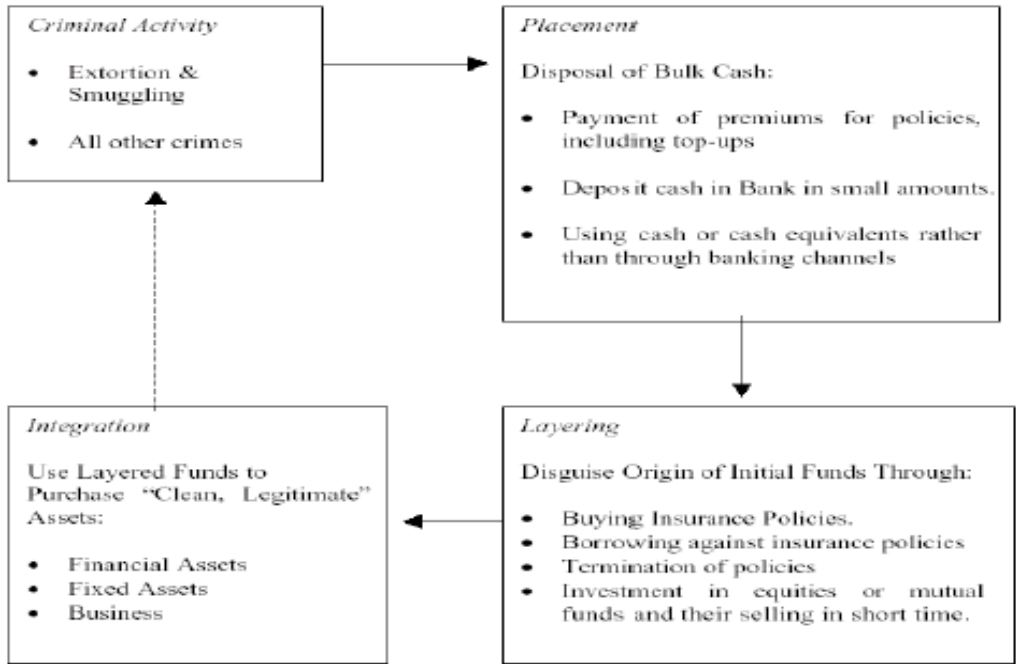
Layering involves converting the proceeds of crime into another form and creating complex layers of financial transactions to hide the original source. It also involves the movement of funds from institution to institution to hide the source and ownership of the funds, conceal the audit trail and break the link with the original crime.

"Integration": Now, having successfully layered the funds at integration stage criminal can invest funds in assets like businesses, house, cars, financial assets, etc.

Thus Integration means the reinvestment of those funds in an apparently legitimate business so that no suspicion of its origin remains and to give the appearance of legitimizing the proceeds.

ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 5 of 20
Document Title: Anti Money Laundering Policy				

Process of Money Laundering



I.2. Money laundering in India

With the growing financial sector, India is vulnerable to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in gems, smuggling, corruption and income tax evasion. Large portions of illegal proceeds are laundered through the

alternative remittance system called "hawala". Under this system, individuals transfer funds from one country to another or from one state to another, often without the actual movement of currency.

I.3 Regulatory Framework

The Government of India has enacted the PMLA, 2002 and issued rules and regulations thereunder ("PMLA") for preventing money laundering and countering the financing of terrorism in India, with effect from July 1, 2005.

The PMLA defines the offence of money laundering as "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually 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 Prevention of Money Laundering Act (PMLA), 2002 brought into force with effect from 1st July 2005 including any statutory reenactment(s) or modification(s) thereof, is applicable to all the financial institutions. The application of anti-money laundering measures has also been emphasized by international regulatory agencies as a key element in combating money laundering. Establishment of anti money laundering programs by financial institutions is one of

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 6 of 20	
Document Title: Anti Money Laundering Policy					

the central recommendations of the Financial Action Task Force (FATF) and also forms part of the Core Principles of the International Association of Insurance Supervisors (IAIS).

Accordingly, PFRDA has set out regulatory guidelines/instructions, including subsequent amendment thereof, to the intermediary registered with PFRDA as part of an Anti-Money Laundering/ Combating the Financing of Terrorism Program. The Policy is about achieving applicable regulatory objectives, accordingly applicable regulations/rules/guidelines/notification issued by concerned regulator from time to time including statutory amendment thereof shall prevail over the policy in case any discrepancy/conflict between Policy and applicable Acts, Rules, and Regulation.

1.4 Scope of applicability:

Aditya Birla Sun Life Pension Management Limited (ABSLPML) is registered with Pension Fund Regulatory and Development Authority as a Pension Fund and assumed the day-to-day investment management activities of the fund under various NPS schemes in accordance with the scheme objectives, Trust Deed, provisions of Investment Management Agreement and PFRDA Regulations & Guidelines.

ABSLPML is also registered with PFRDA to act as Point of Presence (PoP) under NPS architecture and shall perform the functions relating to registration of subscribers, undertaking Know Your Customer (KYC) verification and customer due diligence, receiving contributions and instructions from subscribers and transmission of the same in the NPS architecture.

Therefore, ABSLPML is required to comply with the applicable provision of PFRDA (PoP) Regulations 2018 and the Prevention of Money Laundering Act (PMLA), 2002 & the rules framed thereunder as may be applicable from time to time and reporting & compliance of various activities under PMLA & PFRDA guidelines issued for KYC/AML/CFT.

This AML Policy is applicable to all individuals working in the organisation including directors, Senior Executives, Senior Managers, Officers, employees (whether permanent, fixed-term or temporary including those on deputation), consultants, contractors, trainees, interns and agency staff, agents or any other person associated with our Company and such other persons, all such appointed agents/ business correspondent/POP- sub entity involved in on-boarding NPS Subscribers.

1.4 OBJECTIVES:

The objective of guidelines is to:

- a) Create awareness and provide clarity on Know Your Customer (KYC) standards and AML measures.
- b) Framework for obligations of ABSLPML under PMLA.
- c) To facilitate employees at all levels including persons associated with ABSLPML to align their operations with best practices followed by other Point of Presence Intermediaries/ Pension Fund Industry.
- d) To assist law enforcement agencies in their effort to investigate and track money launderers.

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 7 of 20	
Document Title: Anti Money Laundering Policy					

Important definition:

To better understand certain terms commonly used with reference to AML/ CFT (Combating the Financing of Terrorism) under the PMLA 2022 and other applicable laws are given below:

- i) **“Aadhaar number”**, shall have the meaning assigned to it under clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, hereinafter referred to as “Aadhaar Act”.
- ii) **“Act / PML Act / PMLA”** means the Prevention of Money Laundering Act, 2002.
- iii) **“Authentication”**, means the process as defined under clause (c) of section 2 of the Aadhaar Act.
- iv) **“Central KYC Records Registry”** (CKYCR) means an entity defined under clause (ac) of sub rule (1) of Rule 2 of the PML Rules.
- v) **“Certified copy”** shall mean comparing the copy of officially valid document so produced by the subscriber with the original and recording the same on the copy by the authorised officer of the reporting entity in a manner prescribed by PFRDA.
- vi) **“Client”** shall have the meaning assigned to it under clause (ha) of sub section (1) of Section 2 of the PML Act.
- vii) **“Client Due Diligence”** (CDD) shall have the meaning assigned to it under clause (b) of sub-rule (1) of Rule 2 of the PML Rules.
- viii) **“Designated Director”** shall have the meaning assigned to it under clause (ba) of sub-rule (1) of Rule 2 of the PML Rules.
- ix) **Principal Officer:** is an officer designated by a Reporting Entity for the purpose of Section 12 of PMLA, 2002. Rule 7 of the PML (Maintenance of Records) Rules 2005
- x) **“Digital KYC”** shall have the meaning assigned to it under clause (bba) of sub-rule (1) of Rule 2 of the PML Rules.
- xi) **“Equivalent e-document”** shall have the meaning assigned to it under clause (cb) of sub-rule (1) of Rule 2 of the PML Rules.
- xii) **Suspicious Transactions:** it is defined under Rule 2(g) of the PML Rules and means a transaction whether or not made in cash which to a person acting in good faith:
 - a) Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime: as per schedule A to PMLA; or
 - b) Appears to be made in circumstances of unusual or unjustified complexity; or
 - c) Appears to have no economic rationale or bonafide purpose; or
 - d) Gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 8 of 20	
Document Title: Anti Money Laundering Policy					

- i) **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR.
- ii) **“KYC Identifier”** shall have the meaning assigned to it under clause (cc) of sub-rule (1) of Rule 2 of the PML Rules.
- iii) **“KYC Records”** shall have the meaning assigned to it under clause (cd) of sub-rule (1) of Rule 2 of the PML Rules.
- iv) **“Non-face-to-face customers”** shall have the same meaning assigned to it under sub clause (ix) of 3(b) of Chapter I of Master Direction – Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time.
- v) **“Offline verification”** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar Act.
- vi) **“On-going Due Diligence”** means regular monitoring of transactions to ensure that they are consistent with the subscriber’s profile and source of funds.
- vii) **“Subscriber”** shall have the meaning as per clause (t) of sub-section (1) of section 2 of the PFRDA Act. In these guidelines, the phrase Subscriber, Customer and Client has been used interchangeably and shall be considered to have the same meaning.

I.5 AML Program:

- The Company shall ensure that all employees have a high level of integrity, and that in the exercise of their functions apply the norms established in the system of prevention of money laundering and financing of terrorist activities.
- Laws against money laundering and the financing of terrorism will not only apply to individuals seeking to legitimize funds from illegal activities, but also to financial institutions, insurance, managers of pension funds and the staff involved in such operations.
- The employees of the company identifying suspicious transactions related to money laundering and the financing of terrorism shall report them to their AML Principal Officer.

I.6 ABSLPML Obligations under PMLA, 2002:

Section 12 under Chapter IV places certain obligations on the REs which are as follows:

- a) Maintain a record of all transactions, including information relating to transactions covered under money laundering transaction in such manner as to enable it to reconstruct individual transactions.
- b) Furnish to Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value as may be prescribed.
- c) Verify the identity of its clients in such manner and subject to such conditions as may be prescribed.

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 9 of 20	
Document Title: Anti Money Laundering Policy					

- d) Identify the beneficial owner, in any, of such of its clients, as may be prescribed.
- e) Maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.
- In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing of terrorism, ABSLPML has an AML program, which includes:

- Internal policies, procedures, and controls,
- Designating a Principal Compliance officer,
- Recruitment and training of employees/agents,
- Internal Control/Audit.

ABSLPML has designed an AML program to report suspicious transactions. Weightage is given more on design and implementation of a program, rather than isolated instances failing to report suspicious transactions. The AML program also envisages submission of Suspicious Transaction Reports (STR) to a Financial Intelligence Unit-India (FIU-IND) set up by the Government of India for further investigation and action. Formal instructions on the manner of submission of Suspicious/Cash Transaction Reports (STR/CTR) to the Financial Intelligence Unit are issued by PFRDA. ABSLPML to report all the suspicious transactions to FIU-IND.

II.1. INTERNAL POLICIES, PROCEDURES AND CONTROLS

Know Your Customer (KYC) & Customer Identification.

- The Company shall have internal policies and procedures regarding “Know your customer” to:
 - a) Verify and document the true identity of the customers that establish a relation, open accounts or conduct significant transactions. (Refer Annexure A for the list of KYC documents)
 - b) Obtain and document any additional information on the customer based on the risk per activity.
 - c) Make sure that no business transactions are carried out with companies or persons whose identities cannot be confirmed, failing to provide the required information or that provide false information or containing significant inconsistencies that cannot be satisfied after a further investigation.

Customer’s KYC procedures is divided thus:

- A. Customer Acceptance Procedure (CAP)
- B. Customer Identification Procedure (CIP)
- C. Monitoring transactions
- D. Risk Management

A. CUSTOMER ACCEPTANCE PROCEDURE (CAP)

ABSLPML has adopted a customer acceptance procedure to accept application for onboarding NPS subscribers covering comprehensive Customer Identification Procedure/KYC verification. Customer acceptance Procedure/KYC verification broadly covers:

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 10 of 20	
Document Title: Anti Money Laundering Policy					

- **Customer Due Diligence process (KYC Verification)**

Customer Due Diligence measures comprises the following:

- a) Verification of the client's identity using reliable, independent source documents, data or information
- b) Understand the ownership and control structure of the subscriber.
- c) Conduct ongoing due diligence and scrutiny, i.e., perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the knowledge about the subscriber, its business and risk profile, taking into account, where necessary, the client's source of funds.

KYC compliance and submission of Permanent Account Number (PAN) is mandatory for every client who invests in NPS schemes. Every individual will have to fill up a prescribed uniform KYC application or submit KYC details online in registration journey and support it with documents regarding identity i.e., PAN, proof of address, and a latest photograph.

Customer Due Diligence (KYC verification) shall be done basis on following alternative process/mode as per PML Act 2002 and rules made there under or any modification thereof from time to time.

1. **PAN based verification through NSDL pan data base:**

The customer uploads self-attested KYC documents for identity and address proof including a copy of his/her permanent account number ("PAN Card") and Company will refer to the data base available with National Securities Depository Limited ("NSDL") to verify the client's identity along with other information available in PAN data base and this would suffice as adequate customer due diligence.

2. **Reliance on third party for KYC verification**

The Company will engage qualified third party(s) as per PML Rule 2002 including any statutory modification thereof to carry out the process of verification of KYC subject to complying with Regulation 44 of the PFRDA (Point of Presence) Regulations 2018, if required. Such third party shall be regulated, supervised, or monitored for, and have measures in place for compliance with CDD and recordkeeping requirements in line with the obligations under the PML Act and PFRDA circulars issued in this regard.

ABSLPML may also utilise SEBI KRA for KYC in accordance with PFRDA circular PFRDA/2019/16/PDES/2 dated 23rd September 2019. The ultimate responsibility for relying on third party KYC is with the ABSLPML.

3. **Using of KYC documents of Sponsor Company's customer**

The Company will use the KYC documents of such customer available in the data base of Sponsor Company (Aditya Birla Sun Life Insurance Company Ltd.). This will be subject to (a) the Pension Company retaining the ultimate responsibility customer verification; and (b) express consent of the customer being taken for sharing of KYC documents and data between the ABSLI

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 11 of 20	
Document Title: Anti Money Laundering Policy					

and the Company or any other condition as may be specified by the concerned Authority or applicable regulation.

4. Offline Aadhaar based KYC verification

The Company will use Aadhaar QR code / barcode which contain machine-readable information for offline KYC verification of the customers by using third party QR code reader machine. This will be subject to (i) obtaining the consent of a subscriber (ii) ensuring that we will not subject an Aadhaar number holder to electronic authentication and will not collect, use or store an Aadhaar number or biometric information of any individual for any purpose or any other condition as may be specified under applicable regulation.

PFRDA vide its circular dated April 24, 2020, allowed to utilize Aadhaar based offline paperless KYC verification process which eliminated providing physical copy of Aadhaar. The process of Aadhaar Paperless Offline eKYC based registration is detailed in the customer acceptance Policy.

5. Using Central KYC Record Agency platform to validate the KYC records of subscriber

The Government of India vide their Notification dated November 26, 2015, authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) to act as and to perform the functions of the Central KYC Records. Registry under the said rules, including receiving, storing, safeguarding and retrieving the KYC records under the Prevention of Money-Laundering Act, 2002. CERSAI is a centralized repository of KYC records of customers/investors in the financial sector with uniform KYC norms and inter-usability of the KYC records across the financial sector. Central KYC (CKYC) will store all the customer/investor information at one central server that is accessible to all the financial institutions. After opening a KYC account under the CKYC, customer/investor will get a 14-digit identification number ("KYC Number") and that the same may be quoted by the investor wanting to invest in NPS Schemes.

The Company is registered with CERSAI as reporting entities under under the PML Rules and it will link up with the Central Record Keeping Agency for the purpose of uploading, retrieving and validating the KYC records of subscriber

6. In- person Verification

The Company will complete KYC through an "in person verification" along with scrutiny of identity and address proof of the Customer.

The above Customer Due Diligence practices shall be reviewed and approved by the Board of the Company from time to time as and when required by regulation or the concerned authority.

7. Video Based Customer Identification Process (VCIP)

PFRDA has allowed an alternative (optional) electronic process of Identification/ KYC in paperless form, carried out by it. This process requires seamless, secure, real-time with geotagging, consent based audio-visual interaction with the subscriber to obtain identification information including the necessary KYC documents required for the purpose of client due diligence and to ascertain the veracity of the information furnished by the subscriber.

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 12 of 20	
Document Title: Anti Money Laundering Policy					

- **Knowing existing subscribers**

The AML/ CFT requirements are applicable for all the existing subscribers. Hence, necessary CDD with KYC (as per extant PML Rules) shall be done for the existing subscribers from time-to-time basis the adequacy of the data previously obtained. Further, periodic updation of KYC of NPS account shall be done as follows:

- In case of NPS Tier II accounts (excluding Tier II Tax Saver Scheme) - Every 3 years.
- In case of Tier II account, where subscriber is Politically Exposed Person (PEP) – Every 2 years.
- At the time of exit from NPS Tier I account.
- Whenever there is upward revision in the risk profile of the subscriber.
- As and when there are revision or changes in PML Act / PML Rules.

B. CLIENT IDENTIFICATION PROCEDURE

As mentioned above, ABSLPML shall not accept any application for subscription unless it is accompanied with valid KYC document/ details (in case of online). ABSLPML shall follow the KYC procedure established by PFRDA for the purpose of client identification procedure.

C. MONITORING TRANSACTIONS

C.1. Third Party Payment

NPS contribution amount paid by person other than NPS Subscriber should not be allowed except in following cases:

- Contribution made by a Corporate on behalf of its employees in the employees NPS account out of employer – employee relationship as allowed under the applicable regulation.
- Transfer of superannuation fund into employees' NPS account by Trust. The superannuation fund is created by an employer for its employees under applicable laws and it is created in the name of a Trust to hold and manage the fund for employees.
- Third party payment as allowed by PFRDA or concerned regulator.

C.2. Monitoring Cash Transaction:

NPS contributions must be made through banking channels. No cash transaction is allowed for remittance of contribution in NPS account. As per PMLA, integrally related cash transaction above Rs.10 lakhs to be reported to FIU IND by the 15th of next month.

A. C.3. Monitoring Suspicious Transactions:

It is difficult to define what constitutes a suspicious transaction and a complete list is next to impossible. However, a suspicious transaction will often be one which gives rise to a reasonable suspicion that it may involve the laundering of money or is inconsistent with a customer's known,

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 13 of 20	
Document Title: Anti Money Laundering Policy					

legitimate business or personal activities. An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behavior. **Suspicious transactions also include "Attempted Transactions" which is of suspicious nature.**

a) Identification of suspicious transaction

Adequate procedures are developed, implemented, controlled and enhanced to identify suspicious transactions. When the transactions are inconsistent with risk categorization and updated profile of the subscribers shall be put in to use as a part of effective identification and reporting of suspicious transactions. Accordingly, in the event when a transaction pattern that are unusual to the known relationship with a subscriber and which appearing have no economic rationale must be identified, monitored and adequate CDD and enhanced due diligence as may be required must be conducted for such subscriber.

Identification process of potential suspicious transactions may include unless specifically excluded under any applicable regulations in enforce or concerned regulator:

1. Prospective subscriber insisting on anonymity, reluctance to provide identifying information, or providing minimal seemingly fictitious information.
2. Frequent request for change in addresses (Review of frequency can be decided by the reporting entity based on risk categorisation of subscriber)
3. Transactions which are inconsistent with risk categorization and unusual with known relationship of a subscriber which appear to have no economic rationale.
4. Review of publicly available information including media reports regularly on a "best effort basis" to find names of persons / entities involved in predicate offences.
5. The risk categorization of a subscriber especially high-risk subscriber, transactions of such subscriber residing in countries / territories, or such jurisdiction of a country notified by FATF as having deficiencies in their AML/CFT regime. Any such transactions shall be strictly in compliance with PFRDA (PoP) Regulations, 2018 & and the Guidelines for Operational Activities to be followed by Point of Presence (POPs), or any other applicable guidelines including amendments from time to time.
6. Transactions and patterns of transactions by Politically Exposed Persons (PEPs).
7. Names of subscribers are checked against a list of banned entities issued by Security Council Committee established pursuant to various United Nations' Security Council (UNSC), can be accessed regularly from the United Nations website at "https://www.un.org/securitycouncil/sanctions/1267/ag_sanctions_list" and UNSC be accessed regularly from the United Nations website at <https://www.un.org/securitycouncil/sanctions/1988/materials>".

All steps taken to identify suspicious transactions may be documented for future reference.

C4. Suspicious Transactions Reporting (STR):

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 14 of 20	
Document Title: Anti Money Laundering Policy					

The Company shall once a transaction has been detected and qualified as suspicious by the Compliance Officer; it shall be reported to the authorities designated by Law. At this stage, the interruption of the commercial relation with the customer shall be evaluated.

Adequate procedures are developed, implemented, controlled and enhanced to identify suspicious transactions and to report to FIU-IND setup by the Government of India. Suspicious Transactions are to be reported within 7 days of identification of such suspicious transaction to FIU-IND.

C5. Confidentiality

Directors, officers and employees (permanent and temporary) of ADITYA BIRLA SUN LIFE Pension Management LIMITED shall be prohibited from disclosing the fact that a suspicious Transaction Report or related information of a subscriber/ prospect is being reported or provided to the FIU-IND.

C.6 Verification at the time of exit (superannuation /premature exit / death etc.)

No payments should be made to third parties on attainment of superannuation except payments to nominee(s)/ legal heir(s) in case of death. However, Necessary due diligence of the subscriber(s) / nominee(s) / legal heir(s) should be carried out before making the pay-outs/settling claims.

D. Risk Management

ABSLPML may devise procedures for creating Risk Profiles of their existing and new subscribers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

D1. Risk Assessment:

ABSLPML shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk, severally and together, for subscriber, countries or geographic areas, and products, services, transactions, or delivery channels etc. as prescribed by Authority.

In the context of the very large base of subscribers and the significant differences in the extent of risk posed, ABSLPML shall classify the subscriber into high risk and low risk, based on the individual and profile to decide upon the extent of due diligence. The basic principle enshrined in this approach is that an enhanced client due diligence process for higher risk categories of subscriber's shall be adopted. Conversely, a simplified subscriber's due diligence process may be adopted for lower risk categories of clients.

The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk (viz, high, medium or low) and the appropriate level and type of mitigation to be applied.

Notwithstanding anything contained in above, while assessing the subscriber's risk profile, ABSLPML may consider the following factors:

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 15 of 20	
Document Title: Anti Money Laundering Policy					

- Nature of account (For eg - NPS Tier I, NPS Tier II, NPS Tier II Tax Saver Scheme, NPS Lite, APY and any other scheme regulated/administered by PFRDA)
- Source of contribution
- Mode of contribution (Cash / Online / Cheque / DD/ Card/ employers bank account etc)
- Regularity in the flow of contribution (For eg – Contributions under employer and employee relationship)
- Withdrawals under Tier I and Tier II account
- Residence status of subscriber (For eg – Subscribers residing in jurisdiction with higher national risk assessment)
- Politically Exposed Person
- Contributions made by the subscriber vis-à-vis the declared income/ income range

The above list is indicative and not exhaustive. ABSLPML may consider additional factors using its own judgement and past experience.

D.3. Risk Categorization:

While assessing the subscriber's risk profile under pensions schemes regulated / administered by PFRDA, ABSLPML may inter-alia take into account the following:

- Whether contributions are mandatory contribution viz Employees of central / state government / autonomous bodies / public sector undertakings covered under NPS (These accounts would generally involve lower risk).
- Whether contributions are voluntary and low-contribution: APY being fixed and low contribution pension scheme and NPS Lite being low contribution pension scheme (These accounts generally involve lower risk).
- Contributions towards NPS Tier I account on a voluntary basis (These accounts generally involve moderate risk).
- Voluntary contributions towards NPS Tier II account, which is a withdrawable account (These accounts involve generally higher risk in comparison to other categories)

Risk categorization shall be undertaken based on parameters detailed above besides others like subscriber's identity, nature of employment, high value deposits in Tier II account / in Tier I account near superannuation, unusual withdrawals in Tier II account etc. ABSLPML shall ensure enhanced due diligence (EDD) for NPS Tier II account (except accounts under NPS Tier II Tax Saver Scheme)

D.3. High Risk Profile Subscribers

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 16 of 20	
Document Title: Anti Money Laundering Policy					

Following subscribers considered as high-risk profiles for the purpose of enhanced/higher due diligence.

- (i) Non-resident clients (NRI);
- (ii) High Net worth clients
- (iv) Politically exposed persons (PEP) of foreign origin:
- (v) Current /Former Head of State, Current or Former Senior High-profile politicians and connected persons.
- (vi) Client in high-risk countries.
- (vii) Clients belonging to the countries where corruption/fraud level is high
- (ix) Clients with dubious reputation as per public information available etc.

The above-mentioned list is only illustrative and ABSLPML may exercise independent judgement to ascertain whether any other set of clients shall be classified as high risk profile or not.

D.4. Enhanced Due Diligence (EDD):

ABSLPML shall ensure Enhanced Due Diligence (EDD) where the risk of money laundering or terrorist financing is higher such as the background and purpose of all complexes, unusually large transactions and all unusual pattern of transactions, which have no apparent economic or lawful purpose.

D.2. Simplified Due Diligence (SDD): 'Simplified Due Diligence' shall be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.

However, Simplified Client Due Diligence measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific high-risk scenarios apply, based on the Risk Assessment/categorization policy of the reporting entities.

II.2. DESIGNATED DIRECTOR AND PRINCIPAL COMPLIANCE OFFICER:

The company shall have a Principal Compliance Officer and Designated Director, appointed by the Board or equivalent body, according to the laws of the place where it is established.

The Principal Compliance Officer and Designated Director will be responsible for monitoring the compliance of the system of prevention of money laundering and the financing of terrorism.

Duties of the Principal Compliance Officer

The Principal Compliance Officer will:

1. be the point of contact with FIU-IND with respect to money laundering matters;
2. approve any new or revised procedures for combating money laundering within a business unit;
3. review and investigate any suspicions of money laundering identified by employees, agents and/or Business Unit Compliance Officers;
4. determine when a transaction constitutes a suspicious transaction or large cash transaction requiring reporting to FIU-IND;

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 17 of 20	
Document Title: Anti Money Laundering Policy					

5. file a Suspicious Transaction Report where he is no longer satisfied with the true identity of the customer
6. file a Suspicious Transaction Report for attempts to avoid disclosure of PAN
7. Determine transactions involving receipts by non-profit organizations of value more than Rs. 10 lacs or its equivalent in foreign currency requiring reporting to FIU-IND.
8. ensure cash transaction where forged or counterfeit currency notes or bank notes, if any have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions are reported to FIU-IND as required;
9. maintain a system for reporting suspicious and prescribed transactions to the FIU-IND as required;
10. ensure no transaction (financial or otherwise) is permitted in any fund, contract freeze under Section 51A of UAPA Act;
11. carry out, on a periodic basis, in accordance with the local policy and procedures, an examination of a sample of client transactions to determine whether appropriate anti-money laundering and client identification procedures were followed;
12. Maintain up-to-date information on money laundering laws and regulations and communicate such to relevant stakeholders.

Any change in details of the Designated Director and Principal Officer for AML/ CFT Guidelines shall be communicated to the Regulator and FIU-IND within the timelines prescribed by the Authority.

II.3 RECORD KEEPING

1. In view of Rule 5 of the PML rules, ABSLPML, its Designated Director, Principal Officer, employees are required to maintain the information/records of types of all transactions [as mentioned under Rules 3 and 4 of PML Rules 2005] as well as those relating to the verification of identity of clients for a period of five years.
2. The records referred to in the said Rule 3 shall be maintained for a period of five years from the date of transaction. Records pertaining to all other transactions, (for which insurers are obliged to maintain records under other applicable Legislations/Regulations/Rules) insurers are directed to retain records as provided in the said Legislation/Regulations/Rules but not less than for a period of five years from the date of end of the business relationship with the customer.
3. Records can be maintained in electronic form and/or physical form. In cases where services offered by an appointed POP-SE or business correspondents are utilized, 19.2.1 Insurers shall be satisfied about the organizational capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data.
4. The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored and recorded.
5. The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 18 of 20	
Document Title: Anti Money Laundering Policy					

6. It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.
7. ABSLPML should implement specific procedures for retaining internal records of transactions to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. ABSLPML should retain the records of those contracts, which have been settled by claim or cancelled, for a period of at least five years after that settlement.
8. In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. Wherever practicable, insurers are required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.
9. In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained (physically or electronically) for at least five years after the business relationship is ended.

II.4 ANTI MONEY LAUNDERING TRAINING

The Company shall give priority attention to the periodic training programs for their employees/distribution staff/ processing staff on the Money Laundering and Financing of Terrorism Prevention System.

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff does not forget their responsibilities. Timing and content of training packages for various sectors of staff will need to be adapted. Compliance shall make training module and put to test the employees on ongoing basis.

Department wise records of training imparted to staff in the various categories detailed above shall be maintained. Compliance would do surprise check on those training records.

II.5. INTERNAL AUDIT AND CONTROL

AML Policy should be reviewed as and when prescribed by the Authority (Changes there of shall be incorporated). The same shall be approved by the Board.

Compliance with policies, procedures and controls relating to money laundering activities should be verified on a regular basis by the Internal Audit department.

II.6 OFFICIALLY VALID DOCUMENT

“Officially Valid Document” for the purposes of opening account under National Pension System consists of;

- 1) Passport,

				Security Classification: INTERNAL	
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 19 of 20	
Document Title: Anti Money Laundering Policy					

- 2) Driving licence,
- 3) Permanent Account Number (PAN) Card,
- 4) Voter's Identity Card issued by Election Commission of India,
- 5) Job card issued by NREGA duly signed by an officer of the State Government,
- 6) Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or
- 7) Identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- 8) letter issued by a gazetted officer, with a duly attested photograph of the person.
- 9) Any other document as notified by the Central Government in consultation with the regulator

In addition to the documents mentioned above, few more documents have been added to the identity proof, where simplified measures are applied for verifying the limited purpose of proof of address of the prospective subscribers and where a prospective subscriber is unable to produce any proof of address, the following documents shall be accepted as 'officially valid document.

- (a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, Water bill);
- (b) property or Municipal tax receipt;
- (c) bank account or Post Office savings bank account statement;
- (d) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- (e) letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and licence agreements with such employers allotting official accommodation; and
- (f) documents issued by Government departments of foreign jurisdiction and letter issued by Foreign Embassy or Mission in India".

		Security Classification: INTERNAL		
ABSLPM	Anti Money Laundering	Version 1.2	Date: 20/04/2023	Page 20 of 20
Document Title: Anti Money Laundering Policy				

Annexure A

List of KYC documents required for both entry and exist under National pension System (NPS) which will be subject to compliance with applicable act, rules and regulations or directions received from PFRDA from time to time.

Sl. No.	Proof of Identity (Copy of any one of the given below document)	Proof of Address (Copy of any of the below documents)
1	Passport issued by Government of India	Passport issued by Government of India
2	Ration Card with Photograph	Ration Card with Photograph and residential address
3	Bank Pass book or certificate with Photograph	Bank Pass book or certificate with Photograph and residential address
4	Voters Identity Card with Photograph and residential address	Voters Identity Card with Photograph and residential address
	Valid Driving license with Photogarp	Valid Driving license with Photogarp and residential address
5	PAN card issued by Income Tax Department	Letter from any recognized public authority at the level of Gazetted officer like District Magistrate, Divisionall commissioner BDO, Tehsildar, Mandal Revenue officer, Judicial Magistrate etc.
6	Certificate of identity with photograph signed by a Parliament or Member of Legislative Assembly	Certificate of identity with photograph signed by a Parliament or Member of Legislative Assembly
7	Aadhar Card/Letter issued by Unique Identification Authority of India	Aadhar Card/Letter issued by Unique Identification Authority of India clearly showing the address
8	Job card issued by Government , Defence, Parliamentary and Police Department's	Job card issued by Government , Defence, Parliamentary and Police Department's
	Photo identity card issued by Government , Defence, Parliamentary and Police Department's	Latest Electricity/Water bill in the name of Subscriber /Claimant and showing the address (less than 6 month old)
9	Ex-Service Man Card issued by Ministry of Defence to their employees	Latest Telephone bill in the name of the Subscriber / Claimant and showing the address (less than 3 months old)
10	Photo Credit Card	Latest Property /House Tax receipt (not more than one year old)
		Existing valid registered lease agreement house on stamp paper (in case of rented/ accommodation)

Note:

- a) If the address on the document submitted for identity proof by the propective customer is same as that declared by subscriber in the account opening form, the document may be accepted as a valid proof of both identity and address.
- b) If the address indicate on the document submitted for identity proof differs from the current address mentioned in the account opening form, a seprate proof of address should be obtained.