

# **PREVENTION OF MONEY LAUNDERING (PMLA) POLICY**

## 1. INTRODUCTION :

This Policy has been framed by SBICAP Securities Ltd. (“SSL/Company”) in order to comply with the applicable Anti Money Laundering (AML) Standards/ Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under.

The Prevention of Money Laundering Act, 2002 (PMLA) was brought into force with effect from 1<sup>st</sup> July, 2005. As per PMLA, every banking company, financial institution (which includes chit fund company, a cooperative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA.

For the purpose of PMLA, transactions include:

1. All cash transactions of the value of more than Rs 10 lakhs or its equivalent in foreign currency.
2. All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency, such series of transactions within one calendar month
3. all transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency;
4. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions
5. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non monetary account such as Demat account, security account maintained by the registered intermediary.

For the purpose of suspicious transactions reporting, apart from ‘transactions integrally connected’, ‘transactions remotely connected or related’ need to be considered.

“Suspicious transactions” means a transaction whether or not made in cash which to a person acting in good faith –

1. gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

2. appears to be made in circumstances of unusual or unjustified complexity or
3. appears to have no economic rationale or bonafide purpose.

Pursuant to the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering standards, The Securities and Exchange Board of India, has from time to time issued circulars directing Intermediaries to adopt Strict Customer Due Diligence practices in order to prevent Money Laundering.

SSL being an intermediary in the securities market registered with the Securities and Exchange Board of India is required to adopt and implement a policy for Prevention of Money Laundering as laid down hereunder pursuant to the Prevention of Money Laundering Act, 2005 and the Rules, Regulations and Notifications thereunder as a compliance with Regulatory Requirement.

## **2. POLICY OBJECTIVES:**

- To have a proper Customer Due Diligence (CDD) process before registering individual and non-individual clients (hereinafter also refer to as clients)
- To monitor/maintain records of all cash transactions of the value of more than Rs.10 lacs in foreign currency.
- To maintain records of all series of integrally connected cash transactions within one calendar month.
- To monitor and report suspicious transactions.
- To discourage and identify money laundering or terrorist financing activities.
- To take adequate and appropriate measures to follow the spirit of the PMLA.

## **3. SCOPE :**

To be in compliance with these obligations, SSL is fully committed to establish appropriate policies and procedures for the prevention of Money Laundering and Terrorist Financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

These policies and procedures (with amendments from time to time) apply to all employees of SSL and is to be read in conjunction with the existing guidelines. The following procedures have been established to ensure that all employees know the identity of their customers and take appropriate steps to combat money laundering.

It is obligatory for every employee, at all levels, to go through this Policy, understand the provisions, and co-operate in the implementation of the procedures. For any clarifications on this subject, at any point of time, the employees should contact the

Compliance Officer of the company, who is also designated as the Principal Officer under the Act.

#### **4. IMPLEMENTATION OF THIS POLICY:**

##### **I. PRINCIPAL OFFICER :**

The Company shall designate the Compliance Officer of SSL as the Principal Officer who shall act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Illustrative duties of Principal Officer will be as follows:

- Monitoring the implementation of Anti Money Laundering Policy
- Timely reporting of transactions and sharing of information as required under the law
- Liasoning with law enforcement agencies
- Providing clarifications to staff members on the provisions of the Act, Rules, Guidelines and the policy of the company.

##### **II. DESIGNATED DIRECTOR :**

The Company shall nominate the Whole-time Director & CFO who oversees the operations of the Company including implementation of Prevention of Money Laundering Rules, as the Designated Director of the Company under the Prevention of Money laundering Act, 2002 and Rules framed there under who shall be responsible for ensuring overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

SSL shall communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU-IND.

##### **III. PROCEDURES TO COMBAT MONEY LAUNDERING & TERRORIST FINANCING :**

The Customer Due Diligence Process includes three specific parameters:

**A. Policy for Acceptance of Clients**

**B. Client Identification Procedure**

**C. Other Due Diligence**

**D. Suspicious Transactions identification, monitoring & reporting.**

## A. CUSTOMER ACCEPTANCE POLICY :

The Customer Acceptance norms specified hereinbelow shall be applicable to clients sourced directly by employees of SSL and also with regard to clients sourced through Channel Partners, Feet on Street, Marketing agents, Independent Financial Advisors etc. of SSL.

All persons sourcing clients on behalf of SSL shall be required to adhere to the requirements specified herein below that are aimed to identify the types of clients that are likely to pose a higher than the average risk of money laundering or terrorist financing:

1. **In-person verification:** In person verification (the “IPV”) shall be mandatory for all clients. Accounts shall be opened only for those persons whose in-person verification has been done as per the SEBI/Stock Exchange/Depository or other regulations in this regard. The client should visit the branch of SSL or the authorised official may visit the client at the residence/office to complete the in-per verification procedures.

2. **KYC Procedures:** Accept only clients in respect of whom complete KYC procedures have been completed. Client’s account shall not be opened in case the client fails to submit any required documents as per Customer Identification Policy below:

- a. Documents shall be accepted as per the checklists given from time to time
- b. Photocopies submitted by the clients shall be compulsorily verified with original
- c. All details in the form shall be filled in by the clients without fail
- d. There shall be no compromise on submission of mandatory information – Accounts should not be opened here if the client refuses to provide information/documents.

3. **Benami Accounts:** No account should be opened in a fictitious / benami name or on an anonymous basis.

4. **Debarred Clients:** Before opening of clients accounts, check should be done to verify whether the client’s name matches with names in any of the following lists:

- SEBI Debarred List
- UNSC
- PEP
- OFAC (Office of Foreign Access and Control given by US Treasury Dept.)
- FATF
- Watch out Investors- [www.watchoutinvestors.com](http://www.watchoutinvestors.com)

- NSE Arbitration
- such other list that may be specified by the Regulators/Compliance Department from time to time

Accounts should not be opened of client with known criminal background.

#### **5. Clients of Special Category:**

Due care shall be taken while accepting clients of Special Category.

Clients of Special Category include but shall not be limited to the following-

- i. Non- resident clients
- ii. High net-worth clients
- iii. Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
- iv. Companies having close family shareholdings or beneficial ownership
- v. Politically Exposed Persons (**PEP**)  
(i.e. Individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. and family members or close relatives of PEPs)
- vi. Companies offering foreign exchange offerings
- vii. Clients in high risk countries  
(i.e - where existence / effectiveness of money laundering controls is suspect where there is unusual banking secrecy, countries active in narcotics production- countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent - countries against which government sanctions are applied- countries reputed to be Havens/ sponsors of international terrorism offshore financial centers, tax havens, countries where fraud is highly prevalent.
- viii. Non face to face clients
- ix. Clients with dubious reputation as per public information available etc.

#### **6. Designated Individuals/Entities :**

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <http://www.un.org/sc/committees/1267/consolist.shtml>.

SSL must ensure that accounts are not opened in the name of anyone whose name appears in said list. SSL shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full

details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

### **7. Additional Segment Activation**

For all clients applying for trading rights in the futures and options segments, further details/documents substantiating ownership of Assets would be required. Illustrative list is as follows:

1. Copy of ITR acknowledgement.
2. In case salary income- Salary Slip, Copy of Form 16
3. Copy of demat account holding Statement
4. Networth Certificate
5. Bank Account Statement for the last 6 months
6. Self Declaration with relevant supporting documents

### **Treatment of Accounts of Clients of Special Category :**

**1. NRI:** While opening NRI account utmost care should be exercised. While opening an NRI Repatriable or NRI Non Repatriable inter alia, following documents should be collected from the clients:

NRI Repatriable/Non Repatriable

1. PAN Card Copy
2. Passport Copy
3. Indian Address Proof
4. Cancelled Cheque copy of NRE A/c
5. PIS Permission issued from RBI.
6. NRI Address Proof
7. Bank Statement Copy.
8. Client Master Copy for demat account.
9. Tax Residency proof

**2. High Networth Clients:** High networth clients could be classified as such if at the account opening stage or during the course of the relationship, it is realized that the client's investments or the appetite for investment is high.

**3. Trust, Charity and NGOs:** Both public as well private, registered as well unregistered trust will have to be classified in the Special Category. Any Charitable or Nongovernmental organization or a Non Profit Organization will be also classified herein.

**4 Close family shareholdings or Beneficial Ownership:** In case of close family shareholdings the objective is to understand whether the beneficiaries of two or more accounts, which may also be opened at different times are same, then both need to be marked under this special category.

**5. Politically Exposed Persons:** In case of PEPs, the account should be opened only after consent of the senior management and all the required documents are collected and client should be marked as PEP in records. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship. SSL shall verify the sources of funds of the PEP by obtaining bank statements from time to time.

**6. Company offering foreign Exchanges:** At the account opening stage if the individual or the entity is registered foreign exchange dealer, then the same may be categorized.

**7. Client in High Risk Country:** No accounts shall be opened if received from a client who was residing in a high risk jurisdiction and may have investment proceeds which may have also originated from these countries. The list may be obtained from the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website ([www.fatf-gafi.org](http://www.fatf-gafi.org)).

**8. Client with dubious Public Reputation:** If a client's reputation during the opening of the account or post opening the account is known to be not good, then the same is marked in this special category.

The parameters of risk perception in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc shall be captured at the account opening stage to enable categorization of customers into low, medium and high risk. SSL has indicative categories of customers which would fall into low, medium and high risk categories (**Annexure I**). The list shall be updated with approvals from Compliance and Business groups.

For the purpose of risk categorization, individuals/entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. Illustrative examples of low risk customers are as follows:

- salaried employees whose salary structures are well defined;
- Government Departments and Government owned companies;
- regulators and statutory bodies; etc.

Customers that are likely to pose a higher than average risk to SSL shall be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. SSL shall apply Customer Due Diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.



While the profile of the customer is captured in the account opening form, Client Profile sheet is also prepared at the account opening stage for all accounts (individual / non individual). The Client Profile sheet is an addendum to the account opening form and captures in further detail the profile of the customer, especially the expected transaction pattern of the account.

## **B. CUSTOMER IDENTIFICATION POLICY :**

The following Customer Identification Norms shall be adhered to in respect of all new clients to establish the identity of the client alongwith firm proof of address to prevent opening of account which is fictitious/benami/anonymous in nature.

SEBI/the Stock Exchanges/the Depositories and other regulatory authorities under which SSL is governed from time to time specify various KYC norms/guidelines that have to be adhered to in order to be able to Identify Customers. Such Norms and guidelines should be followed scrupulously at the time of customer acceptance.

Further given below is a list of Basic Requirements to be obtained from Individual and non-individual clients at the time of account opening.

### **Proof of Identity (POI):**

Every client would be identified based on only photo identity as prescribed under applicable KYC norms. The PAN Card, which is compulsory, would also serve as a photo identity. Other Identity proofs which might be collected for verification are as under:

- I. Passport
- II. Voter ID Card
- III. Driving license
- IV. PAN card with photograph
- V. Unique Identification Number (UID) (Aadhar Card)
- VI. Identity card/document with applicant's Photo, issued by a) Central/State Government and its Departments, b) Statutory/Regulatory Authorities, c) Public Sector Undertakings, d) Scheduled Commercial Banks, e) Public Financial Institutions, f) Colleges affiliated to Universities (**this can be treated as valid only till the time the applicant is a student**), g) Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members, and h) Credit cards/Debit cards issued by Banks.

### **Proof Of Address (POA):**

The address of the Client would be verified from one of the following:

- I. Ration card
- II. Passport

- III. Voter ID Card
- IV. Driving license
- V. Bank passbook / Bank Statement
- VI. Unique Identification Number (UID) (Aadhar Card)
- VII. Verified copies of a) Electricity bills (**not more than three months old**), b) Residence Telephone bills (**not more than three months old**) and c) Leave and License agreement / Agreement for sale.
- VIII. Self-declaration by High Court & Supreme Court judges, giving the new address **in respect of their own accounts.**
- IX. Identity card/document with address, issued by a) Central/State Government and its Departments, b) Statutory/Regulatory Authorities, c) Public Sector Undertakings, d) Scheduled Commercial Banks, e) Public Financial Institutions, f) Colleges affiliated to Universities (**this can be treated as valid only till the time the applicant is a student**) and g) Professional Bodies such as ICAI, ICWAI, Bar Council etc., to their Members.

**In case of Non-Individuals, additional documents to be obtained from non-individuals, over & above the POI & POA, as mentioned below:**

Types of entity	Documentary requirements
Corporate	<ul style="list-style-type: none"> <li>• Copy of the balance sheets for the last 2 financial years (to be submitted every year).</li> <li>• Copy of latest share holding pattern including list of all those holding control, either directly or indirectly, in the company in terms of SEBI takeover Regulations, duly certified by the company secretary/Whole time director/MD (to be submitted every year).</li> <li>• Photograph, POI, POA, PAN and DIN numbers of whole time directors/two directors in charge of day to day operations.</li> <li>• Photograph, POI, POA, PAN of individual promoters holding control - either directly or indirectly.</li> <li>• Copies of the Memorandum and Articles of Association and certificate of incorporation.</li> <li>• Copy of the Board Resolution for</li> </ul>

	<p>investment in securities market.</p> <ul style="list-style-type: none"> <li>• Authorised signatories list with specimen signatures.</li> </ul>
<b>Partnership firm</b>	<ul style="list-style-type: none"> <li>• Copy of the balance sheets for the last 2 financial years (to be submitted every year).</li> <li>• Certificate of registration (for registered partnership firms only).</li> <li>• Copy of partnership deed.</li> <li>• Authorised signatories list with specimen signatures.</li> <li>• Photograph, POI, POA, PAN of Partners.</li> </ul>
<b>Trust</b>	<ul style="list-style-type: none"> <li>• Copy of the balance sheets for the last 2 financial years (to be submitted every year).</li> <li>• Certificate of registration (for registered trust only).</li> <li>• Copy of Trust deed.</li> <li>• List of trustees certified by managing trustees/CA.</li> <li>• Photograph, POI, POA, PAN of Trustees.</li> </ul>
<b>HUF</b>	<ul style="list-style-type: none"> <li>• PAN of HUF.</li> <li>• Deed of declaration of HUF/ List of coparceners.</li> <li>• Bank pass-book/bank statement in the name of HUF.</li> <li>• Photograph, POI, POA, PAN of Karta.</li> </ul>
<b>Unincorporated association or a body of individuals</b>	<ul style="list-style-type: none"> <li>• Proof of Existence/Constitution document.</li> <li>• Resolution of the managing body &amp; Power of Attorney granted to transact business on its behalf.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>

<b>Banks/Institutional Investors</b>	<ul style="list-style-type: none"> <li>• Copy of the constitution/registration or annual report/balance sheet for the last 2 financial years.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Foreign Institutional Investors (FII)</b>	<ul style="list-style-type: none"> <li>• Copy of SEBI registration certificate.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Army/ Government Bodies</b>	<ul style="list-style-type: none"> <li>• Self-certification on letterhead.</li> <li>• Authorized signatories list with specimen signatures.</li> </ul>
<b>Registered Society</b>	<ul style="list-style-type: none"> <li>• Copy of Registration Certificate under Societies Registration Act.</li> <li>• List of Managing Committee members.</li> <li>• Committee resolution for persons authorised to act as authorised signatories with specimen signatures.</li> <li>• True copy of Society Rules and Bye Laws certified by the Chairman/Secretary</li> </ul>

**SSL shall carry out Know Your Client for Eligible Foreign Investors as per the category specified below**

Category	Eligible Foreign Investors
I	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies
II	a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance / Reinsurance Companies, Other Broad Based Funds etc. b) Appropriately regulated entities such as Banks, Asset

	<p>Management Companies, Investment Managers/ Advisors, Portfolio Managers etc.</p> <p>c) Broad based funds whose investment manager is appropriately regulated</p> <p>d) University Funds and Pension Funds</p> <p>e) University related Endowments already registered with SEBI as FII/Sub Account</p>
III	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

List of KYC Documents to be obtained for Eligible Foreign Investor as defined above as per its category:

Document Type		Category - I	Category - II	Category - III
<b>Entity Level</b>	Constitutive Docs	Required	Required	Required
	Proof of Address	Required Power of Attorney, mentioning the address, is acceptable as address proof	Required Power of Attorney, mentioning the address, is acceptable as address proof	Required - Address proof other than Power of Attorney should be submitted.
	PAN Card	Required	Required	Required
	Financials	Exempt	Exempt	Risk based - Financial data sufficient.
	SEBI Registration Certificate	Required	Required	Required
	Board Resolution	Exempt	Required	Required
	KYC Form	Required	Required	Required
<b>Senior Management (Whole Time Directors/ Partners/</b>	List	Required	Required	Required
	Proof Of Identity	Exempt	Exempt	Entity declares on letterhead - full name,

<b>Trustees/ etc.)</b>				nationality and DoB OR Photo-identity proof'
	Proof of Address	Exempt	Exempt	Declaration on letter head
	Photographs	Exempt	Exempt	Exempt
<b>Authorized Signatories</b>	List & Signatures	Required - List of Global Custodian ('GC') signatories can be given in case of POA to GC	Required - List of GC signatories can be given in case of POA to GC	Required
	Proof Of Identity	Not required	Not required	Required
	Proof of Address	Not required	Not required	Not required
	Photographs	Not required	Not required	Required
<b>Ultimate Beneficial Owner ('UBO')</b>	List	Exempt	Required - Can declare "no UBO over 25%"	Required
	Proof Of Identity	Exempt	Exempt	Required
	Proof of Address	Exempt	Exempt	Exempt
	Photographs	Exempt	Exempt	Exempt

### **Basic KYC Norms to be followed for verification/ scrutiny**

a) The photograph in the PAN card and in any other address proof which contains a photograph must match. This should be followed to ensure that no account is opened in anonymous or fictitious names.

b) As per SEBI, Depository, Exchange guidelines, all Address and Identification proofs, should be verified with the originals by any of the employee of SSL. Care should be taken that the employee, who is verifying the copies of the proofs, should be competent to do the same.

- c) In-Person verification of Applicant (s) made compulsory as per Exchanges and Depository norms should be done by an employee of SSL only or as specified by the Regulators from time to time. The person conducting verification should visit the address provided by the applicant (s) and complete in person verification.
- d) Proof should be collected for both permanent address and correspondence address and the same should be verified with originals.
- e) Notwithstanding the above, the Company should prohibit doing business with any individual or entity whose identity cannot be determined or who refuses to provide information or who have provided information that contains significant inconsistencies which cannot be resolved after due investigation.
- f) Verify whether any of the existing Client or new Applicant, falls within the UN sanction list and/ or is debarred by SEBI from dealing in securities. In this case, if any of the existing Client falls in either of the categories, the said Client would be suspended from trading immediately & the matter would be reported to the concerned Regulatory Authority if required. In case of new applicant falling within the category, such account should not be opened. Clients name in the regulatory orders issued by the exchanges on a day to day basis should be barred from trading with immediate effective.
- g) In case of Non Resident clients, remittance only from authorized banking channels will be accepted.
- h) Clients should not be activated to trade in derivative segment unless the clients submit a valid proof of financial information.

### **C. OTHER DUE DILIGENCE:**

- Any communication in respect of the Client shall be with the Client only.
- Trade Orders/Instructions shall be accepted from the Client only.
- In case the client wishes to authorise a third party to give trade orders/instructions to the company in the client's account, a duly notarized Power of Attorney/Proxy Letter shall be provided by the Client and KYC documents like Proof of Identity, Proof of Address and Relationship with the client of such authorised person shall be obtained.
- Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party

other than the client, that party shall be identified using Customer Identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. Understand the ownership and control structure of the client; The client identification criteria to be followed for various categories of non-individual as per SEBI Circular dated Jan 24, 2013 ; CIR/MIRSD/2/2013 is given below :

In case of Company, Partnership or Unincorporated Association/Body of Individuals, the Intermediary:

SSL shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

- i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
- ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

b. In cases where there exists doubt under clause (a) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

c. Where no natural person is identified under clauses (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

**In case client is a trust:**

SSL shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the



settler of the trust, the trustee, the protector, the beneficiaries with 15% 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.

**Exemption in case of listed companies:**

Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

**In case client is foreign investors:**

for the purpose of identification of beneficial ownership of the foreign investors' viz., Foreign Institutional Investors, SSL shall identify beneficial owners with shareholding or beneficial interest in the client equal to or above 25%. If Global Custodian /Local Custodian provides an undertaking to submit these details, then SSL shall take such undertaking only. In this context SSL shall rely on the clarifications issued by SEBI vide it's circular CIR/MIRSD/11/2012 dated September 5, 2012.

- 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 registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and

The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

KYC carried out by KYC Registration Agencies registered with SEBI shall be accepted as a valid KYC for onboarding a client provided due process in relation to the same under the regulations are followed.

**Monitoring transactions and ongoing due diligence and scrutiny**

At regular interval, ongoing due diligence and scrutiny shall be conducted 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 Organization's knowledge of the client, its business and risk profile, taking into account, where necessary, the customer's source of funds.

SSL shall apply higher levels of due diligence when an account is operated by a Power of attorney holder or where an account is opened by an intermediary in fiduciary

capacity. KYC documents will be taken for both the mandate holder/intermediary in fiduciary capacity and the account holder.

#### **Periodicity of Updation of documents obtained during account opening :**

- KYC exercise to be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Full KYC includes all measures for confirming identity and address and other particulars of the customer that the SSL considers necessary based on the risk profile of the customer.
- KYC exercise including but not limited to Positive confirmation (obtaining KYC related updates through e-mail / letter / etc/Website updation) for confirming identity & address & other particulars of client.
- The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

#### **D. SUSPICIOUS TRANSACTIONS IDENTIFICATION, MONITORING& REPORTING**

- (i) The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his/her reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.
- (ii) While determining suspicious transactions, SSL shall be guided by definition of suspicious transaction contained in the Rules as amended from time to time.
- (iii) An indicative list of suspicious activities contained is provided along with this policy. (**Annexure II**)
- (iv) While ensuring that there is no tipping off to the customer at any level, SSL may put restrictions on operations in the accounts where an STR has been made.

#### **Suspicious transactions reporting to Financial Intelligence Unit-India (FIU-IND)**

In terms of the Rules, SSL shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address or any other address as may be specified by FIU from time to time:

Director, FIU-IND, Financial Intelligence Unit-India,  
6th Floor, Hotel Samrat, Chanakyapuri,  
New Delhi -110021, India  
Website: <http://fiuindia.gov.in>

#### **IV. MAINTENANCE OF RECORDS OF TRANSACTIONS / INFORMATION TO BE PRESERVED / MAINTENANCE AND PRESERVATION OF RECORDS**

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the PMLA Act. In terms of the Rules, the provisions of PMLA Act, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on financial institutions in regard to preservation and reporting of customer account information.

##### **Maintenance of records of transactions :**

SSL shall have a system of maintaining proper record of all transactions including records of all transactions prescribed under Rule 3 of the Rules, as mentioned below:

(a) all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

(b) all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;

(ba) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;

##### **Information to be preserved:**

SSL shall maintain and preserve the following information in respect of transactions referred to in Rule 3 of the Rules including all necessary information specified by the regulator to permit reconstruction of individual transactions in respect of transactions referred to in Rule 3 of the Rules:

(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.

##### **Retention of Records**

SSL shall take appropriate steps to 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.

**SSL shall observe following document retention terms:**

SSL shall maintain and preserve a records for a period of five years from the date of transaction between SSL and the client, all necessary records of transactions, both domestic or international, which will 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 persons involved in criminal activity.

SSL shall maintain and preserve the record of documents evidencing the identity of its clients and beneficial owner (e.g. copies or records of official identification documents like passport, identity cards, driving licenses or similar documents) as well as accounts file and business correspondence for a period of five years after the business relationship between a client and SSL has ended or the account has been closed whichever is later.

SSL shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the Company or until it is confirmed that the case has been closed.

**V. FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES :**

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA. Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism.

The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

Accordingly, the aforesaid obligations shall be followed by SSL to ensure the effective and expeditious implementation of said Order has been issued vide SEBI Circular ref. no: ISD/AML/CIR-2/2009 dated October 23, 2009.

## VI. CUSTOMER EDUCATION / EMPLOYEES' TRAINING / EMPLOYEES'HIRING :

Implementation of KYC procedures requires SSL to demand certain information from customer which may be of personal nature or which has hitherto never been called for. This sometimes leads to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Team Leaders/ Relationship Managers shall explain to the customers the regulatory requirements and benefits of adhering to the KYC guidelines and seek co-operation of the customer.

SSL shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC/AML procedures and fully understand the rationale behind the KYC/AML policies and implement them consistently.

Further, Compliance department should periodically sensitize the staffs with regards to compliance norms and the amendments in law from time to time.

KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse our infrastructure. It should therefore, be necessary that adequate screening mechanism is put in place by the Company as an integral part of their recruitment / hiring process of personnel. The Human Resources department confirms the previous employment details given by the employee with prior employer. Further, SSL account of the employee is compulsorily required to be opened with SSL, which is subject to the KYC requirements of SSL.

## VII. REVIEW :

The policy and procedures on the prevention of anti money laundering and terrorist financing shall be reviewed annually to ensure their effectiveness in accordance with regulatory changes.

Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures.

**ANNEXURE I**
**RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF INDIVIDUALS**

<b>Type</b>	<b>Recommended Risk Categorisation</b>	<b>Risk Perception</b>
Salaried	Low risk	Source on income is fixed and pattern of entries in the account can be correlated with known sources of income/ expenditure.
Senior citizens	Medium / High Risk	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O
House-wife	Medium / High Risk	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O
Self Employed- Professionals/ Businessmen	Low risk (except professionals associated with the film industry who will be categorized as "Medium" risk).	Accounts maintained by Chartered Accountants, Architects, Doctors, Lawyers, Sportsmen, etc.
Non Resident Individuals	Low / Medium risk	Transactions are regulated through AuthoriseDealers and the accounts are opened only after IPV. In case an IPV is not performed and we have relied on documentation submitted by the client, the account would be categorised as medium risk.
Politically Exposed Persons resident	High Risk	Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign

outside India	<p>country, e.g. Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category</p> <p>intending to establish a relationship and check all the information available on the person in the public domain. Front end staff should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Such accounts should be subjected to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members and close relatives of PEPs. Further SSL may maintain a list of additional accounts as “Designated PEP”</p> <p>The accounts of Politically Exposed Persons resident outside India shall be opened only after obtaining the approval of Business Head. Further, in the event of an existing customer or the beneficial owner of an account subsequently becoming PEP, Business head approval would be required to continue the</p> <p>business relationship and such accounts would be subjected to Customer Due Diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. In such events SSL shall be guided by the information provided by the clients or front end teams.</p>
---------------	--

**NOTE:** If any of the above accounts are operated by Power of Attorney (POA) holder/mandate holder, then the account will be categorized as “High Risk”.

## RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF NON-INDIVIDUALS

Risk categorization of Non Individual customers can be done basis:

A. Type of Entity                      B. Industry; C. Country of Domicile

### **A. Type of Entity**

<b>Type</b>	<b>Recommended Risk Categorisation</b>	<b>Risk Perception</b>
Private Ltd/Public Ltd Companies	Low / Medium / High risk	Depending on the clarity of the shareholding structure and the nature of operations, such companies would be classified.
Local Authorities or Public Bodies	Low Risk	These types of entities are governed by specific Acts, Notifications etc framed by the Government of India or the State Govt and are controlled and run by the Govt.
Mutual Funds/Scheduled Commercial Banks/Insurance Companies/Financial Institutions	Low Risk	These entities are strictly regulated by their respective regulators.
Partnership Firm	Low / Medium / High risk	Depending on the clarity of the shareholding structure and the nature of operations, such entities would be classified. Such classifications shall be decided post the review of the compliance officer
Trusts - Public Charitable Trust	Medium / High Risk	Depending on the clarity of the beneficial ownership and the nature of operations, such entities would be classified. Such classifications shall be decided post the review of the compliance officer
Hindu Undivided Family (HUF)	Medium Risk	These are unregistered bodies and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.



Societies / Associations / Clubs	High Risk (except 'Housing Societies' which will be categorized as "Low" risk).	These are not highly regulated entities and the pattern of entries in the account may not be correlated with known sources of income/expenditure.
Trusts - Private Trust	High Risk	These may be unregistered trusts and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.
Co-operative Banks	High Risk	These are not highly regulated entities.

### B & C. Basis Industry and Country of Domicile

Risk Category	Industry	Country of Domicile
High	<p>The Risk categorisation is dependent on industries which are inherently High Risk or may exhibit high cash intensity, as below:</p> <ul style="list-style-type: none"> <li>Arms Dealer</li> <li>Money Changer</li> <li>Exchange Houses</li> <li>Gems / Jewellery / Precious metals / Bullion dealers (including sub-dealers)</li> <li>Real Estate Agents</li> <li>Construction</li> <li>Offshore Corporation</li> <li>Art/antique dealers</li> <li>Restaurant/Bar/casino/night club</li> <li>Import/Export agents (traders; goods not used for own manufacturing/retailing)</li> <li>Share &amp; Stock broker</li> <li>Finance Companies (NBFC)</li> <li>Transport Operators</li> <li>Auto dealers (used/ reconditioned vehicles/motorcycles)</li> <li>Scrap metal dealers</li> <li>Liquor distributorship</li> <li>Commodities middlemen</li> <li>Co-operative Banks</li> <li>Car/Boat/Plane dealerships/brokers</li> <li>Multi Level Marketing (MLM) Firms</li> </ul>	

Medium	None	NA
Low	All other industries	NA

**Notes:**

1. Higher Risk Categorization derived from either A or B or C shall be the applicable risk categorization for the account.
2. Lowering of risk classification shall be carried out by the Compliance officer in consultation with the Chief Risk Officer. This shall be done only where adequate justifications can be provided and the same are mentioned along with the account opening form.
3. Such justifications shall be reviewed 3 months from the date of account opening / first transaction in order to ensure that the classification is proper.

## ANNEXURE II :

### AN INDICATIVE LIST OF SUSPICIOUS ACTIVITIES:

Whether a particular transaction is suspicious or not will depend upon the background details of the client, details of the transactions and other facts and circumstances. Followings are the circumstances, which may be in the nature of suspicious transactions: -

- a. Clients whose identity verification seems difficult or clients appears not to co-operate;
- b. Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- c. Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
- d. Substantial increases in business volume without apparent cause;
- e. Unusually large cash deposits made by an individual or business;
- f. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- g. Transfer of investment proceeds to apparently unrelated third parties;
- h. Off market transactions in the DP account of the clients;
- i. High trading activity in the relatively illiquid scrips;
- j. Major trading activity in the Z and TtoT category scrips;
- k. Options trading / trading in illiquid scrips wherein client has booked unusual profit or loss which does not commensurate with the changes in the prices of underlying security in the cash segment.
- l. High exposures taken by client as compared to income levels informed by clients.
- m. Unusual transactions by "High risk status" and businesses undertaken by shell corporations offshore banks / financial services, businesses reported to be in the nature of export-import of small items.
- n. Synchronized Cross and Self Trades - Scrutinize Synchronized, Self/Cross Trade Report generated by the system/provided by Exchange.
- o. Clients whose turnover is disproportionate with the annual income/Networth provided in KYC.
- p. High value transactions in a new or dormant account
- q. Client offered false or forged identification documents
- r. Adverse media report about criminal activities of Client
- s. Adverse media report about TF or terrorist activities of Client
- t. Client provides inconsistent information
- u. Client could not explain source of funds

- v. Transaction is unnecessarily complex
- w. Transaction has no economic rationale
- x. Transaction inconsistent with Client Profile
- y. Alert raised by Business Associate
- z. Alert raised by other institution, subsidiaries or business associates including cross-border referral