SAMUNNATI FINANCIAL INTEMEDIATION & SERVICES PRIVATE LIMITED

KYC & AML POLICY 2016

VERSION 1

This policy is made as per the RBI circular RBI/2015-16/108 DNBR (PD) CC No. 051/03.10.119/2015-16 dated 1st July 2015.

I. 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards

Introduction

The 'Know Your Customer' guidelines were issued in February 2005 revisiting the earlier guidelines issued in January 2004 in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). These standards have become the international benchmark for framing Anti Money Laundering and combating financing of terrorism policies by the regulatory authorities. Compliance with these standards by the banks/financial institutions/NBFCs in the country have become necessary for international financial relationships. The Department of Banking Operations and Development of Reserve Bank had issued detailed guidelines to the banks based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary. These guidelines are equally applicable to NBFCs. All NBFCs were, therefore, advised to adopt the same with suitable modifications depending on the activity undertaken by them and ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of the Board.

2. General Guidelines

The information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes. Samunnati Financial Intermediation & Services Private Limited (SFISPL) should ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his /her consent and after opening the account.

3. Definitions

3.1 Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with SFISPL and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.2 Designated Director

"Designated Director" means a person designated by the SFISPL to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. In case of SFISPL, the Designated Director is Mr. S.G. Anil Kumar (Director & CEO).

The Principal Officer should not be nominated as the "Designated Director".

3.3 Officially valid document (OVD)

OVD means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, or any other document as notified by the Central Government in consultation with the Regulator.

3.4 Person

In terms of PML Act a 'person' includes:

(i) an individual,

(ii) a Hindu undivided family,

(iii) a company,

(iv) a firm,

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

(vi) every artificial juridical person, not falling within any one of the above persons (i to v), and

(vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).

3.5 Transaction

"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

i. opening of an account;
ii. deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
iii. the use of a safety deposit box or any other form of safe deposit;
iv. entering into any fiduciary relationship;
v. any payment made or received in whole or in part of any contractual or other legal obligation; or
vi. establishing or creating a legal person or legal arrangement.

4. The guidelines are equally applicable to the persons authorised by SFISPL including brokers/agents etc.

5. SFISPL is required to put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months. SFISPL should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. Accordingly, SFISPL is required to undertake 'Client Due Diligence' and apply such measures to existing clients based on risk categorization.

a) SFISPL would need to continue to carry out on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.

b) Full KYC exercise will be required to be done at least every two years for high risk individuals and entities.

c) Full KYC exercise will be required to be done at least every ten years for low risk and at least every eight years for medium risk individuals and entities taking in to account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained. Physical presence of the clients may, however, not be insisted upon at the time of such periodic updations.

d) Fresh photographs will be required to be obtained from minor customer on becoming major.

6. KYC/AML guidelines issued by the RBI shall also apply to SFISPL branches and majority owned subsidiaries located outside India, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. In case, there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of SFISPL are required to adopt the more stringent regulation of the two.

7. Allocation of Unique Customer Identification Code

In the context of recommendations of Working Group constituted by the Government of India regarding the introduction of unique identifiers for customers across different Financial Institutions for setting up a centralized KYC Registry, non-deposit taking NBFCs with asset size of Rs. 25 crore and above and all Deposit taking NBFCs have been advised to allot UCIC while entering into new relationships with individual customers as also the existing customers. A Unique Customer Identification Code (UCIC) will help NBFCs to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable NBFCs to have a better approach to risk profiling of customers. SFISPL shall allot a Unique Customer Identification Code to every customer.

8. Accounts of Politically Exposed Persons (PEPs)

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. SFISPL should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on such person in the public domain. SFISPL should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in the SFISPL Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an on-going basis. The above norms should also be applied to the accounts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, SFISPL should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

The instructions are also applicable to accounts where PEP is the ultimate beneficial owner. Further, in regard to PEP accounts, SFISPL should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner.

9. Client accounts opened by professional intermediaries

When SFISPL has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. SFISPL may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. SFISPL also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at SFISPL and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at SFISPL, SFISPL should still look through to the beneficial owners.

If SFISPL decides to accept an account in terms of the Customer Acceptance Policy, SFISPL should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. Therefore, under the extant AML/CFT framework, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients.

Therefore, SFISPL should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that

inhibits SFISPL ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

10. Accounts of proprietary concerns

SFISPL should take reasonable measures to identify the beneficial owner(s) and verify his / her / their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is /are.

Accordingly, apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, SFISPL should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

i) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.

ii) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department. SFISPL may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.

iii) The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities.

iv) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

v) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

11. Beneficial ownership

When SFISPL identifies a customer for opening an account, it should identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

(a) Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

(b) Where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

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

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

(e) Where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, 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.

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

12. Principal Officer

SFISPL should appoint a senior management officer to be designated as Principal Officer and the role and responsibilities of the Principal Officer have been detailed therein. With a view to enable the Principal Officer to discharge his responsibilities, the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information. Further, SFISPL should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors. The role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended form time to time.

The Principal Officer for SFISPL is Mr. Ritesh Nair (Head – Compliance & Internal Control).

13. Suspicion of money laundering/terrorist financing

With a view to preventing SFISPL from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing, whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, SFISPL shall carry out full scale customer due diligence (CDD) before opening an account.

14. Filing of Suspicious Transaction Report (STR)

SFISPL should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. In the circumstances, if SFISPL believes that it would no longer be satisfied that it knows the true identity of the account holder, the Company should also file an STR with FIU-IND.

Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in terms of Rules notified thereunder

1. SFISPL to appoint a Principal Officer and put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. In this connection, Government of India, Ministry of Finance, Department of Revenue, issued a notification dated July 1, 2005 in the Gazette of India, notifying the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the SFISPL in regard to preservation and reporting of customer account information.

With the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

"If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

(a) issue a warning in writing; or

(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

2. Maintenance of records of transactions

2.1 SFISPL should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

(iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions;

(iv) all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

SFISPL is required to adhere to the reporting requirements as per the amended rules.

2.2 SFISPL is required to maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it was denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction.

3. Preservation of records

SFISPL should 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.

(i) In terms of PML Amendment Act 2012, SFISPL should maintain for at least five years from the date of transaction between the SFISPL 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.

(ii) SFISPL should ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills, etc.) obtained while opening the account and during the course of business

relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification of records and transaction data should be made available to the competent authorities upon request.

(iii) SFISPL may maintain records of the identity of their clients, and records in respect of transactions referred to in Rule 3 in hard or soft format.

(iv) SFISPL is required to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors to scrutinize the transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for five years as is required under PMLA, 2002.

4. Reliance on third party due diligence

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, SFISPL may rely on a third party subject to the conditions that-

1. SFISPL immediately obtains necessary information of such client due diligence carried out by the third party;
2. SFISPL takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
3. SFISPL is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;
4. the third party is not based in a country or jurisdiction assessed as high risk and
5. SFISPL is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable

5. Reporting to Financial Intelligence Unit-India

5.1 In terms of the PMLA rules, NBFCs are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,

Financial Intelligence Unit-India,

6th Floor, Hotel Samrat,

Chanakyapuri,

New Delhi-110021

(i) There are altogether five reporting formats prescribed for SFISPL viz. i) Manual reporting of cash transactions ii) Manual reporting of suspicious transactions iii) Consolidated reporting of cash transactions by Principal Officer of the SFISPL iv) Electronic data structure for cash transaction reporting and v) Electronic data structure for suspicious transaction reporting which are enclosed to this circular. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. SFISPL should initiate urgent steps to ensure electronic filing of cash transaction report (CTR) as early as possible. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof were furnished in the instructions part of the concerned formats. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, SFISPL should scrupulously adhere to the following:

(a) The cash transaction report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, individual transactions below rupees fifty thousand may not be included. Cash transaction reporting by branches/offices of SFISPL to their Principal Officer should invariably be submitted on monthly basis (not on fortnightly basis) and the Principal Officer, in turn, should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule;

(b) The Suspicious Transaction Report (STR) should 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 should record his reasons for treating any transaction or a series of transactions as suspicious. It should 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 should be made available to the competent authorities on request;

(c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;

(d) Utmost confidentiality should be maintained in filing of CTR and STR with FIU-IND. The reports may be transmitted by speed/ registered post, fax, email at the notified address;

(e) It should be ensured that the reports for all the branches are filed in one mode i.e. electronic or manual;

(f) A summary of cash transaction report for the SFISPL as a whole may be compiled by the Principal Officer of the SFISPL in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted both for manual and electronic reporting.

5.2. SFISPL to initiate steps to ensure electronic filing of cash transaction report (CTR) and Suspicious Transaction Reports (STR) to FIU-IND. In case where all the branches are not yet fully computerized, the Principal Officer should cull out the transaction details from branches

which are not computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in.

5.3. SFISPL may not put any restrictions on operations in the accounts where an STR has been made. However, it should be ensured that there is no tipping off to the customer at any level. It is likely that in some cases, transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. SFISPL should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

5.4. In regard to CTR, the cut-off limit of Rupees ten lakh is applicable to integrally connected cash transactions also. Further, after consultation with FIU-IND, it is clarified that:

a) For determining integrally connected cash transactions, SFISPL should take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month. However, while filing CTR, details of individual cash transactions below rupees fifty thousand may not be indicated. Illustration of integrally connected cash transactions is furnished as below.

Illustration of Integrally connected cash transaction

The following transactions have taken place in an NBFC during the month of April, 2008:

Date	Mode	Dr. (in Rs.)	Cr. (in Rs.)	Balance (in Rs.)
				BF - 8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000	1,00,000.00	3,90,000.00
Monthly summation		10,10,000.00	6,00,000.00	

i) As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs.10 lakhs. However, the NBFC should report only the debit transaction taken place on 02/04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the NBFC, which is less than Rs.50, 000/-.

ii) All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by NBFC.

b) CTR should contain only the transactions carried out by the SFISPL on behalf of their clients/customers excluding transactions between the internal accounts of the SFISPL.

c) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND immediately in the format (Counterfeit Currency Report – CCR). Electronic data structure has been furnished to enable NBFCs to generate electronic CCRs. These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

The multiple data files reporting format were replaced by a new single XML file format as provided in the 'Download' section of the FIU-IND website (http://fiuindia.gov.in/). All NBFCs were requested to carefully go through the revised reporting format and initiate urgent steps to build capacity to generate reports, which are compliant with the new reporting XML format specifications.

FIU-IND had advised vide their letter F.No.9-29/2011-FIU-IND dated August 28, 2012, that all NBFCs should initiate submission of reports on the FINnet Gateway in 'TEST MODE' from August 31, 2012 to test their ability to upload the report electronically. Such submission in 'Test Mode' was to be continued till FIU-IND informs the NBFCs about 'go-live' of the project.

As the project has gone 'live' NBFCs were advised to discontinue submission of reports in CD, using only FINnet gateway for uploading of reports in the new XML reporting format. Any report in CD will not be treated as a valid submission by FIU-IND. For any clarification / assistance regarding submission of reports, NBFCs may contact FIU-IND help desk at email or telephone numbers 011-24109792/93.

5.5 While making STRs, NBFCs should be guided by the definition of 'suspicious transaction' as contained in Rule 2(g) of Rules ibid. NBFCs should make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

5.6 In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation.

6. SFISPL is required to prepare a profile for each customer based on risk categorization. SFISPL as a part of transaction monitoring mechanism, were required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transactions.

7. SFISPL is required to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. These records are required to be preserved for ten years as is required under PMLA, 2002. Such records and related

documents should be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

8. Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Amendment Rules, 2009/10 - Obligation of banks/Financial institutions

9. Assessment and Monitoring of Risk

SFISPL should have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk, adopting a risk-based approach. As a corollary, SFISPL would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating.

SFISPL should place to put in place a system of periodic review of risk categorization of customers and updation of customer identification data in a time-bound manner.

III. Combating financing of terrorism

In terms of PMLA Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. SFISPL to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

1. SFISPL should ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website. SFISPL should ensure that before opening any new account, the name/s of the proposed customer does not appear in the list. Further, NBFCs should 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 should immediately be intimated to RBI and FIU-IND.

2.Adequate screening mechanism is put in place by SFISPL as an integral part of their recruitment/hiring process of personnel.

3. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, SFISPL may consider an indicative list of suspicious activities.

4. Countries which do not or insufficiently apply the FATF recommendations

Financial Action Task Force (FATF) has issued several Statements on risks arising from the deficiencies in AML/CFT regime of various countries for example Uzbekistan, Iran, Pakistan,

Turkmenistan, Sao Tome and Principe on etc. which are updated from time to time. All NBFCs/RNBCs were required to consider the information contained in the statements issued by FATF which however, does not preclude financial institutions from legitimate trade and business transactions with the countries and jurisdictions mentioned in the statement.

NBFCs should take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. NBFCs should, in addition to FATF Statements circulated by Reserve Bank from time to time, also consider publicly available information for identifying such countries, which do not or insufficiently apply the FATF Recommendations. NBFCs should give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in these countries.

5. Monitoring

Ongoing monitoring is an essential element of effective KYC procedures. SFISPL should examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents be retained and made available to Reserve Bank/other relevant authorities, on request.

SFISPL should apply enhanced due diligence measures on high risk customers. Some illustrative examples of customers requiring higher due diligence are given in the paragraph under reference. In view of the risks involved in cash intensive businesses, accounts of bullion dealers(including sub-dealers) and jewelers should also be categorized by SFISPL as 'high risk' requiring enhanced due diligence.

Ongoing monitoring is an essential element of effective KYC procedures. SFISPL is also required to subject these 'high risk accounts' to intensified transaction monitoring. High risk associated with such accounts should be taken into account by SFISPL to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-ND.

V. Inter-Governmental Agreement (IGA) with United States of America (US) under Foreign Accounts Tax Compliance Act (FATCA) - Registration

Government of India has now advised that to avoid withholding tax, Foreign Financial Institutions (FFIs) in Model 1 jurisdictions, such as India, need to register with IRS and obtain a Global Intermediary Identification Number (GIIN) before January 1, 2015. The FFIs who have registered but have not obtained a GIIN should indicate to the withholding agents that the GIIN is applied for, which may be verified by the withholding agents in 90 days. In this regard, the FAQ published on the IRS website (updated as on December 22, 2014), as received from the Government of India, is furnished in the circular DNBR.CC.PD.No.010/03.10.01/2014-15, dated January 9, 2015. Accordingly, SFISPL may take action appropriately.

VI. Constitution of Special Investigating Team – sharing of information

SFISPL should ensure that the information/documents required by the SIT are made available as and when required.

15. As per the RBI AML Circular dated 1st July 2015 (DNBR (PD) CC No. 051/03.10.119/2015-16) all NBFCs are advised that before opening any new account, it should be ensured that the name/s of the proposed customer does not appear in the list. PFB the link used to download the file for regular update.

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

16. The customer should past the below link as part of the initial checks at the pre-sanction/application stage itself so that no transactions are done with these persons/entities. This is the United States Specially Designated Nationals and Blocked Persons List (OFAC list). The link is given below to check for regular updates.

https://www.treasury.gov/resource-center/sanctions/SDN-List/pages/default.aspx

Customer Identification Procedure

1. For Individuals

(i) Passport*
(ii) PAN card
(iii) Voter's Identity Card issued by Election Commission*
(iv) Driving License*
(v) Job Card issued by NREGA duly signed by an officer of the State Govt
(vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number.*

Documents marked as * can be used as both ID and Address proof. All documents should be valid and not expired as on the date of acceptance.

2. For Companies

(a) Certificate of incorporation;
(b) Memorandum and Articles of Association;
(c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and
(d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

3. For Partnership Firms

(a) Registration certificate;
(b) Partnership deed; and
(c) An officially valid document in respect of the person holding an attorney to transact on its behalf.

4. For Trusts and Foundations

(a) Registration certificate;
(b) Trust deed; and
(c) An officially valid document in respect of the person holding a power of attorney to transact on its behalf.

5. For Proprietorship Concerns

Apart from Customer identification procedure as applicable to the proprietor (take ID and Address proof as applicable for individuals) additionally, take any two of the following documents in the name of the proprietary concern.

- Registration certificate (in the case of a registered concern)
- Certificate/licence issued by the Municipal authorities under Shop & Establishment Act,
- Sales and income tax returns
- CST/VAT certificate
- Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
- Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities.

Operational Procedure to be followed by NBFCs for e-KYC exercise

The e-KYC service of the UIDAI is be leveraged by NBFCs through a secured network. Any NBFC willing to use the UIDAI e-KYC service is required to sign an agreement with the UIDAI. The process flow to be followed is as follows:

1. Sign KYC User Agency (KUA) agreement with UIDAI to enable the NBFC to specifically access e-KYC service.

2. NBFCs to deploy hardware and software for deployment of e-KYC service across various delivery channels. These should be Standardisation Testing and Quality Certification (STQC) Institute, Department of Electronics & Information Technology, Government of India certified biometric scanners at NBFC branches as per UIDAI standards. The current list of certified biometric scanners is given in the link below :http://www.stqc.gov.in/sites/upload_files/stqc/files/UID_Auth_Certlist_250613.pdf

3. Develop a software application to enable use of e-KYC across various NBFC branches, as per UIDAI defined Application Programming Interface (API) protocols. For this purpose, NBFCs will have to develop their own software under the broad guidelines of UIDAI. Therefore, the software may differ from NBFC to NBFC.

4. Define a procedure for obtaining customer authorization to UIDAI for sharing e-KYC data with the NBFC. This authorization can be in physical (by way of a written explicit consent authorising UIDAI to share his / her Aadhaar data with the NBFC for the purpose of opening deposit account) / electronic form as defined by UIDAI from time to time.

5. Sample process flow would be as follows:

a. Customer walks into branch of NBFC with his / her 12-digit Aadhaar number and explicit consent and requests to open a deposit account with Aadhaar based e-KYC.

b. NBFC representative manning the branch enters the number into NBFC's e-KYC application software.

c. The customer inputs his / her biometrics via a UIDAI compliant biometric reader (e.g. fingerprints on a biometric reader).

d. The software application captures the Aadhaar number along with biometric data, encrypts this data and sends it to UIDAI's Central Identities Data Repository (CIDR).

e. The Aadhaar KYC service authenticates customer data. If the Aadhaar number does not match with the biometrics, UIDAI server responds with an error with various reason codes depending on type of error (as defined by UIDAI).

f. If the Aadhaar number matches with the biometrics, UIDAI responds with digitally signed and encrypted demographic information [Name, year / date of birth, Gender, Address, Phone and email (if available)] and photograph. This information is captured by NBFC's e-KYC application and processed as needed.

g. NBFC's servers auto populate the demographic data and photograph in relevant fields. It also records the full audit trail of e-KYC viz. source of information, digital signatures, reference number, original request generation number, machine ID for device used to generate the request, date and time stamp with full trail of message routing, UIDAI encryption date and time stamp, NBFCs decryption date and time stamp, etc.

h. The photograph and demographics of the customer can be seen on the screen of computer at NBFC branches for reference.

i. The customer can open deposit account subject to satisfying other account opening requirements.

Indicative list of High/Medium Risk Customers

Characteristics of High Risk Customers

1. Individuals and entities listed in various United Nations Security Council Resolutions (UNSCRs) such as UN 1267 etc.

2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities.
3. Individuals or entities in watch lists issued by Interpol and other similar international organizations.
4. Customers with dubious reputation as per public information available or commercially available watch lists.
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high risk.
6. Customers conducting their business relationship or transactions in unusual circumstances such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
7. Customers based in high risk countries / jurisdictions or locations
8. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
9. Non-resident customers and foreign nationals.
10. Embassies/consulates
11. Off-shore (foreign) corporation/business
12. Non face-to-face customers
13. High net worth individuals
14. Firms with “Sleeping partners”
15. Companies having close family shareholding or beneficial ownership
16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale.
17. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.
18. Investment Management/ Money Management Company/ Personal Investment Company
19. Accounts for “gatekeepers” such as accountants, lawyers or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
20. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.

21. Trusts, charities, NGOs/Non- Profit Organisations (NPOs) (Especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
22. Money Service Business: including seller of : Money Orders/ Travelers' Checks/ Money Transmission/ Chek Cashing/ Currency Dealing or Exchange
23. Business accepting third party cheques (except Super markets or retail stores that accep payroll cheques/ cash payroll cheques)
24. Gambling/ Gaming including "Junket Operators" arranging gambling tours.
25. Dealers in high value or precious goods (e.g. Jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)
26. Customers engaged in business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries.)
27. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
28. Customers that may appear to be Multi level marketing companies etc.

Characteristics of Medium Risk Customers

1. Non-Bank Financial Institution
2. Stock brokerage
3. Import/Export
4. Gas Station
5. Car/Boat/ Plane dealership
6. Electronics (wholesale)
7. Travel Agency
8. Used Car sales
9. Telemarketers
10. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
11. Dot-com company or internet business
12. Pawn shops

13. Auctioneers
14. Cash intensive business such as restaurants, retail shops, parking garages, fast food stores, movie theaters etc.
15. Sole Practitioners or Law Firms (small, little known)
16. Notaries (small, little known)
17. Secretarial Firms (small, little known)
18. Accountants (small, little known firms)
19. Venture Capital companies

Indicative List of High/Medium risk Products & Services

1. Electronic funds payment services such as Electronic cash (e.g. stored value and payroll cards) Fund transfers (domestic and international) etc.
2. Electronic banking
3. Private banking (domestic and international)
4. Trust and asset management services
5. Monetary instruments such as Travelers' Cheque
6. Foreign Correspondent accounts
7. Trade Finance (such as letter of credit)
8. Special use of concentration accounts
9. Lending activities, particularly loans secured by cash collateral and marketable securities
10. Transactions undertaken for non-account holders (occasional customers)
11. Provision of safe custody and safety deposit boxed
12. Currency Exchange transactions
13. Project financing of sensitive industries in high risk jurisdictions
14. Trade Finance services and transactions involving high risk jurisdictions
15. Services offering anonymity or involving third parties
16. Services involving banknote and precious metal trading and delivery
17. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

Indicative List of High/Medium risk Geographies

Countries/Jurisdictions

1. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions (UNSCR)
2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/TF) risks (www.fatf-gafi.org)
3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
4. Tax havens or countries that are known for highly secretive banking and corporate law practices
5. Counties identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
6. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them
7. Countries identified by credible sources as having significant levels of criminal activity
8. Countries identified by the bank as high risk because of its prior experiences, transaction history or other factors (e.g. legal considerations, or allegations of official corruption)