PMLA POLICY

Shriram Credit Company Ltd Version 1.0.2 Dated October 2018

Policy on Anti Money Laundering

In compliance with the Circular issued by the RBI regarding 'Know Your Customer' guidelines & 'Anti-Money Laundering Standards' to be followed by all NBFCs, the following KYC & PMLA policy of the company has been adopted by the Board of Directors of the Shriram Credit Company Ltd.

Background

Money Laundering (ML) is the processing of criminal proceeds in order to disguise their illegal origin. In response to the international community's growing concern about this problem, most global organizations and National Governments who are the members of the United Nations General Assembly have been actively pursuing programs to deter Money Laundering.

RBI, in tune with Prevention of Money Laundering Act 2002 provided guidelines for NBFC on Anti Money Laundering Standards.

Basic purpose of these guidelines is to prevent money laundering in any form viz.terrorist financing or drug trafficking etc., particularly through some categories of non-individual clients. Such RBI circulars, guideline and acts is applicable to Shriram Credit Company Limited as a Non Banking Financial Company (NBFC).

DEFINITION OF MONEY LAUNDERING

Section 3 of PMLA Act has defined the "offence of money laundering" as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it is untainted properly shall be guilty of offence of money laundering". Such procedures should include inter alia, the following specific parameters which are related to the overall **'Customer Due Diligence Process'**:

- Policy for acceptance of **Customer**
- Procedure for identifying the **Customer**
- Record Keeping and Retention of Records
- Risk Based Approach
- Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)
- Type of Information required to be furnished.
- Time Limit prescribed by the ` Financial Intelligence Unit-India (FIU-IND)'.

PMLA POLICY

Shriram Credit Company Ltd Version 1.0.2 Dated October 2018

- Employee Training
- Customer Education
- Designated officer for reporting of Suspicious Transactions

Policy for acceptance of Customer

- No loan given in a fictitious / benami name or on an anonymous basis. Factors of risk perception (in terms of monitoring suspicious transactions) of the customer are clearly defined having regard to Customer's location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters should enable classification of Customer into low, medium and high risk. Customer of special category may, if necessary, be classified even higher. Such Customers require higher degree of due diligence and regular update of Know Your Customer (KYC) profile.

- Documentation requirement and other information to be collected in respect of different classes of customers depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI from time to time.
- Ensure that an Investment is not accepted or loan disbursed where the Company is unable to apply appropriate customer due diligence measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the customer, information provided to us is suspected to be non genuine, perceived non cooperation of the customer in providing full and complete information. The company should not continue to do business with such a person and file a suspicious activity report. It should also evaluate whether there is suspicious trading in determining in whether to freeze or close the account.
- The circumstances under which the customer is permitted to act on behalf of another person / entity should be clearly laid down. It should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity / value and other appropriate details. Adequate verification of a person's authority to act on behalf the customer should also be carried out.
- Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the customer does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide. For verification of that please check the following website.

Site for checking: http://www.un.org/sc/committees/1267/consolist.shtml

Customers of Special category

The company should be careful while accepting customers of special category like Trust, Charities, NGOs, Politically Exposed Persons (PEP).

Procedure for identifying the Customer

The 'Know your Customer (KYC) policy should clearly spell out the customer identification procedure and due diligence to be carried out at different stages i.e. while establishing the business relationship, in course of subsequent transactions with the customer or when the Company has doubts regarding the veracity or the adequacy of previously obtained customer identification data. Such due diligence will also involve correctly profiling the customer in the account opening forms covering the following:

i. Occupation
ii. PAN
iii. Correspondence & Permanent address
iv. Bank a/c
v. Income details etc.

At the time of opening the account we obtain the different types of proofs:

- Identity proof: PAN has become the sole identity proof for doing any activity in the any financial sector. To obtain PAN as identity proof we makes the following procedures:
  Checking the genuineness of the PAN from "incometaxindiaefiling.gov.in/challan/enterpanforchallan.jsp" which is the authorized site of Income Tax Department, Govt of India. Verify the PAN with original by obtaining the "In person verification" stamp with employee code & signature. Taking the self signature of the client (with stamp in case of non individual customer) and also verify the photograph with the actual photo provided by the customer. In case of non individual client the PAN copy of the entity along with that of the authorized person(s) is also collected. The verification procedures should be same as above.

- Address proof: While collecting the address we follow the RBI guidelines and it is also verified with original. In addition to this the proof should be self certified by customer (with stamp in case of non individual customer).

- Photograph: The photograph affixed in the form should be of the identical person for whom in-person verification has been done.

- Email & Mobile: The email and mobile submitted in the KYC are also to be individually verified.

- Income & occupation: We collect and scrutiny the client income information, occupation (viz. salaried, businessman etc.) with the relevant proof (where applicable) as required under RBI Regulation.

- For Non-individual clients: For corporate client apart from Company's MOA,AOA , Board Resolution, Annual Report and Shareholding pattern we also obtain ID proof and address proof of directors/authorized signatories in case of companies, Partners in case of Partnership firms and Karta in case of HUF while opening the account. Any one of the authorized signatories has to come in person to open account. Other signatories are verified by our branch in charge by visiting their office. We also check the DIN of Director from MCA website.

Record Keeping and Retention of Records

- To comply with the record keeping requirements contained in the PMLA, 2002 as well as other relevant legislation, Rules, Regulations, and Circulars.

- Maintaining such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

- Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, the Company should retain the following information for the accounts of their customers in order to maintain a satisfactory audit trail:

- the beneficial owner of the account;
- the volume of the funds flowing through the account; and
- for selected transactions:

i. the origin of the funds;
ii. the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
iii. the identity of the person undertaking the transaction;
iv. the destination of the funds;
v. the form of instruction and authority.

- Ensure that all customers and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the PMLA 2002, other relevant legislations, Rules and Regulations or circulars.

- Maintain updated list of individuals / entities which are subject to various sanctions / measures pursuant to United Nations Security Council Resolutions (UNSCR), available from the URL https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list (referred to as designated individual / entities) in electronic form. Ensure before accepting any new investment or disbursing new loan that the name of the proposed customer does not appear in the list of designated individuals / entities.

- 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. In the event of matching any particulars of designated individuals / entities, inform the full particulars of the funds, financial assets or economic resources or related services held in the form of securities, within 24 hours to the Joint Secretary (Internal Security-I) Ministry of Home Affairs, at a given fax / phone number and email id. In the event of matching the details beyond doubt, prevent the persons from conducting any further financial transactions under intimation to the Joint Secretary (Internal Security-I) Ministry of Home Affairs, at a given fax/phone number and email id.

- File Suspicious Transactions Reporting to Financial Intelligence Unit-India, covering all transactions

- The following document retention terms should be observed:
    1) All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002) and other legislations, Regulations or circulars.
    2) Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the same period.

- In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

Risk Based Approach

In order to ensure efficient implementation of the AML framework by regularity authority, it is necessary to establish a risk-based process on the basis of business activity of the intermediary. It is recognized that a higher level of due diligence and monitoring would be specified for business areas prone to higher money laundering risk.

Accordingly, individuals and entities whose identities and sources of wealth can be easily identified may be categorized as low risk (example: customer with well defined salary structures).Further, customers that are likely to pose a higher than average risk to SISBL may be categorized as medium or high risk depending on factors such as customer's backgrounds, nature and location of activity etc. (example: clients in high risk countries i.e. where fraud is highly prevalent or sponsors of international terrorism like Dubai, Afghanistan etc., client of special category(CSC) or introduced by CSC).

Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

- Ensure to take appropriate steps to enable suspicious transactions to be recognised and have appropriate procedures for reporting suspicious transactions.

- Any suspicion transaction should be immediately notified to the Money Laundering Control Officer or any other designated officer of the company. The notification may be done in the form of a detailed report with specific reference to the customers, transactions and the nature /reason of suspicion.

- The Company shall report information relating to suspicious transactions to the Director. Financial Intelligence Unit-India (FIU-IND) at the following address; or to the address which may prescribe hereafter:

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

Identification process of Suspicious Transactions:

A transaction can be identified as suspicious from the following way from documents departments report:

- Daily turnover report (which include synchronized/high volume/square up trades).
- Fortnightly demat transaction report.
- Weekly High value cheque bounces report.
- Weekly High value DD/PO/Banker's cheque payment report and
- Monthly turnover report.

Monitoring of Suspicious Transactions:

All this report of suspicious transactions will go to Investment Committee & Compliance department for their perusal. One copy of this report should reach to Principal Officer within the next 2 working day.

Internal audit department will conduct exhaustive checking of KYC and annexed documents of all suspicious clients as well as CSC clients within next working day. Similarly A/Cs, Delivery, DP & Risk department will also give report to Principal Officer regarding whether they have noticed any irregularities in transactions done by CSC and these suspicious clients will be rescruitinised by Internal Audit department. The statement of accounts & other audit trials of transactions will also be checked on a sample basis by Internal Audit and report will be given to Mr. Amit Sankar Gupta and Mr. Adbhut Shankar Pathak who will in turn have a meeting and brief the Principal Officer. Any serious issue is to be highlighted to the Principal Officer immediately.

On the basis of these reports necessary action will be taken by Principal Officer including filing of suspicious report. Necessary steps will also be initiated for closure of account. A report containing all transaction exceeding Rs. 10 lacs which are not in the normal flow of business should come to Principal Officer for his scrutiny. No Bank Draft/PO/Bankers Cheque will be accepted from CSC as it will have no audit trial of customer's source of fund like A/C payee cheque.

Type of Information required to be furnished

The company is required to furnish information about-

- all cash transactions of the value of more than rupees ten lakhs;

- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs where such series of transactions have taken place within a month;

- all cash transactions were 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;

- all suspicious transactions whether or not made in cash

Time Limit prescribed by the ` Financial Intelligence Unit-India (FIU-IND)'

- Rule 8 of the rules notified by notification No.9/2005 (as amended by Notification No.15/2005 and 4/2007) prescribes time limit for furnishing information to the Director, FIU-IND

- The time limit for furnishing information about cash transactions and integrally connected cash transactions to Director, FIU-IND is 15th day of the succeeding month.

- All cash transactions were forget 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 should be furnished to the Director, FIU-IND not later than seven working days from the date of occurrence of such transactions.

- All suspicious transactions have to be furnished to the Director, FIU-IND not later than seven working days on being satisfied that the transactions are suspicious.

Employee Training

Adequate ongoing programme shall be conducted for all employees of front office staff, back office staff, compliance staff, risk management staff and staff dealing with new customers.

The AML training programme shall address the requirements relating to the following:

- Meaning of money laundering.
- Identification of suspicious transactions.
- AML requirements.
- Possible risk of not adhering to the AML requirements.
- Requirements for adequate AML procedures.
- Methods of recognition of suspicious transactions or suspicious behavior of a client.
- Reporting system of suspicious transactions.

Training must relate to employees' daily work and complete from business including continuous training needs.

Customer Education

Shriram Credit Company Ltd shall educate the clients on the objectives of KYC/AML relate program by the following way:

- Preparation of specific literature/pamphlets.
- Hosting AML related seminar organized & lead by management of Shriram Credit Company Ltd in different venue.

Designated officer for reporting of Suspicious Transactions

As per PAML Act the Company shall appointed one Principal Officer as central reference point.

In addition to the Principal Officer and /or any other appointments to be made as per the provisions of the PMLA Act, the company has designated Mr.Amit Sankar Gupta, Mr.Adbhut Shankar Pathak along with the Company Secretary and CFO for regular review of the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness.