SONATA FINANCE PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC), ANTI MONEY LAUNDERING (AML) & COMBATING FINANCING OF TERRORISM (CFT) POLICY

Version	Date of Approval / Reviewal
V.1	30-07-2015
V.2	24-02-2018
V.3	30-05-2019
V.4	22-09-2020

Preamble

In compliance with the Circular issued by the Reserve Bank of India ("RBI") regarding 'Know Your Customer' guidelines & 'Anti-Money Laundering Standards' to be followed by all NBFCs, the following KYC & PMLA policy of Sonata Finance Pvt. Ltd. (hereinafter referred to as the "the Company") to be adopted by the Board of Directors of the Company. This policy is prepared in line with the RBI guidelines.

Background

The Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) 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 both by the banks/financial institutions, including MFIs, has become necessary for international financial relationships. The Reserve Bank of India(RBI) has issued revised set of comprehensive 'Know Your Customer' Guidelines to all Non-Banking Financial Companies (NBFCs), Miscellaneous Non-Banking Companies and Residuary Non-Banking Companies in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and combating financing of terrorism (CFT) policies by the regulatory authorities and advised all NBFCs to adopt the same with suitable modifications depending on the activity undertaken by them and ensure that a proper policy framework on KYC and AML measures are formulated and put in place with the approval of their respective Boards.

Objectives, Scope and Application of the Policy

The primary objective is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities

- To lay down explicit criteria for acceptance of customers
- To establish procedures to verify the bona-fide identification of individuals for commencement of financial relationship.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

SONATA FINANCE PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC), ANTI MONEY LAUNDERING (AML) &

COMBATING FINANCING OF TERRORISM (CFT) POLICY

A.Know Your Customer' Standards

KYC procedures also enable NBFCs to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The Company has framed its KYC policies incorporating the following four key elements:

(i) Customer Acceptance Policy;

(ii) Customer Identification Procedures;

(iii) Monitoring of Transactions; and

(iv) Risk management.

For the purpose of KYC policy, a 'Customer' may be defined as:

- a person or entity that maintains a loan account and/or has a business relationship with the Company;
- one on whose behalf the account is maintained (i.e. the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company.

1. Customer Acceptance Policy (CAP)

The Company's Customer Acceptance Policy, which lays down explicit criteria for acceptance of customers, ensures the following aspects of the customer relationship.

(i) No account is opened in anonymous or fictitious/ benami name(s);

(ii)The Company will define parameters of risk perception. For this purpose, nature of business activity location of customers, mode of payment, annual household income, social and financial status may be taken into account. Given the nature of our business – small ticket loans to low income, informal and financially excluded families are provided, the Company will classify its customer in the following categories:

Low – Medium – High Risk

It is highly unlikely that the Company will have any medium / high risk clients given its focus on the lower income section of society, but for information, examples of customers requiring higher due diligence may include non-resident customers, politically exposed persons (PEPs) of foreign origin, non-face to face customers, and those with dubious reputation as per public information available, etc.

(iii)Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;

(iv)THE COMPANY will not disburse loans to customer where it is unable to apply appropriate customer due diligence measures, i.e. where the Company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-co-operation of the customer or non-reliability of the data/information furnished. However, the Company will have suitable built-in safeguards to avoid harassment of the customer.

(v) Checks against any notified list of the NBFC or the RBI any other regulator, before accepting a customer, to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.

(vi) Field Officers of the Company will ensure to record the Customer's accurate information such as Name, Husband's Name along with Client's Mother's or Father's Name, House No., Village, Post Office, Block/Tehsil, District, Pin Codes etc. as appearing in the identity and Address Proof produced before him.

The Company will prepare a profile for each new customer which may contain information relating to the customer's identity, social/financial status, nature of business activity, information about clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing the customer profile, the Company will seek only such information from the customer which is relevant and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purposes.

It is important to bear in mind that the adoption of Customer Acceptance Policy and its implementation will not result in denial of the Company's services to the general public, especially to those who are financially or socially disadvantaged.

2. Customer Identification Procedure (CIP)

The Company will follow clear NBFC guidelines on the Customer Identification Procedure to be carried out at different stages, i.e. while establishing a financial relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying her identity by using reliable, independent source documents, data or information. The company shall obtain the following information from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner:

a) From an individual who is eligible for enrolment of Aadhaar, the Aadhaar number; the Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time;

Provided, where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained.

"Explanation- Obtaining a certified copy shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the Company"

(b) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have current address, an OVD shall be obtained from the customer for this purpose.

"Provided that in case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

The customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents. The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

The Company for Individual customers, the Company will obtain sufficient identification data to verify the identity of the customer, her address/location, and also her recent photograph. As per the provisions of Rule 9 (17) of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the company shall mandatorily obtain the Aadhar of the client for the identification purpose. The other documents for verification, which can be taken from the customer in addition to Aadhar shall consist of any one of the following - Voter ID Card, PAN Card, Passport, Job Card issued by NREGA, Driving Licence, Ration Card.

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision.

The Prevention of Money Laundering Rules, 2005 and as amended in 2013required every banking company, and financial institution, to identify the beneficial owner and take all reasonable steps to verify his identity.

Beneficial Owner (BO)

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

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

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

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 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.

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. the Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, the Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps are taken to verify the founder managers/ directors and the beneficiaries, if defined.

The Company is vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. The Company examines the control structure of the entity,

determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

CDD procedure, including Aadhaar authentication and obtaining PAN/ form 60 as applicable, shall be carried out for all the joint account holders.

Illustrative nature of the documents required to be produced are enclosed in the Annexure 1.

3. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. However, the extent of monitoring will depend on the risk sensitivity of the customer.

Since the Company does not have any deposit accounts of its customers, this situation will hardly arise, but the Company will in any case pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose or transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. The Company will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. The Company will ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002 (and the Amended Act, 2009). It will also ensure that transactions of suspicious nature and/or any other type of transaction notified under section 12 of the PML Act, 2002 (and the Amended Act, 2009), is reported to the appropriate law enforcement authority.

4. Risk Management

The Company shall follow the risk-based approach wherein the customers shall be categorised as low, medium or high-risk categories. It shall be based on the parameters viz. customers identity, social/financial status, nature of business activity and information about the customers business and their location etc. The Company has to ensure that an effective KYC program is in place and has established appropriate procedures and is overseeing its effective implementation. The program should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has to be explicitly allocated within the Company to ensure that the Company's policies and procedures are implemented effectively. The Company, in consultation with board, has to devise procedures for creating Risk Profiles of their existing and new customers and applied various Anti Money Laundering measures keeping in view the risks involved in a transaction or banking/business relationship.

The Company's internal audit and Risk team functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The Risk department provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

The Company should ensure that internal audit machinery and Risk management team are staffed adequately with individuals who are well-versed in such policies and procedures. The compliance in this regard is to put up before the Audit Committee of the Board on quarterly intervals.

The Company should have an ongoing employee training programme to ensure that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. Further an adequate screening mechanism as an integral part of its personnel recruitment/hiring process shall be ensured.

5. Customer Education

The implementation of KYC procedures requires the Company to demand certain information from customers, which may be of personal nature, or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company has to create adequate awareness among the customers as to the need for adherence to KYC norms through appropriate guidelines in the website. The Company's front line staffs have to be clearly instructed to personally discuss this with customers and if required, the Company has to prepare specific literature/ pamphlets, etc. so as to educate the customer on the objectives of the KYC program. Detailed records of due diligence undertaken shall be kept.

6. Introduction of New Technologies

The Company shall pay adequate attention to any money laundering and financing of terrorism threats that may arise from new or developing technologies and it shall ensure that appropriate KYC procedures issued from time to time are duly applied before the introduction of new products/services/ technologies. The Company neither has deposit accounts nor is permitted by RBI of its customer therefore many of risks presented by the introduction of new technology such as internet banking, mobile banking or transaction that do not require physical presence of the parties etc. are not faced by it. However, the Company pays special attention to any money laundering threats that may arise from new or developing technologies including internet and mobile banking, on-line transactions that might favour anonymity, and take measures, if needed, to prevent its use in money laundering schemes.

As per guidelines issued by RBI following are the important Software Application control and risk mitigation measures that the Company has implemented:

- Each application should have an owner which will typically be the concerned business function that uses the application
- Some of the roles of application owners include:
  - Prioritizing any changes to be made to the application and authorizing the changes.
  - Deciding on data classification/de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/statutory requirements.
  - Ensuring that adequate controls are built into the application through active involvement in the application design, development, testing and change process
  - Ensuring that the application meets the business/functional needs of the users

- Ensuring that the information security function has reviewed the security of the application
- Taking decisions on any new applications to be acquired / developed or any old applications to be discarded
-Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements
- Ensuring that the Change Management process is followed for any changes in application
- Ensuring that the new applications being purchased/developed follow the Information Security policy
- Ensuring that logs or audit trails, as required, are enabled and monitored for the applications

- All application systems should be tested before implementation in a robust manner regarding controls to ensure that they satisfy business policies/rules of the Company and regulatory and legal prescriptions/requirements. Robust controls should be built into the system and reliance on any manual controls has been minimized. Clear instructions should be issued to ensure the audit trails and the specific fields that are required to be captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.

- The Company has to incorporate information security at all stages of software development to improve software quality and minimize exposure to vulnerabilities. Besides business functionalities, security requirements relating to system access control, authentication, transaction, authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are clearly specified at the initial stages of system development/acquisition. A compliance check against the Company's security standards and regulatory/statutory requirements should be put in place.

- All application systems need to have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard.

- Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, must provide for detailed audit trails/ logging capability.

- The audit trails need to be stored as per a defined period as per any internal/regulatory/statutory requirements and it is to be ensured that they are not tampered with.

- Access should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties has to be enforced.

- There should be controls on updating key 'static' business information like customer master files, parameter changes, etc.

- Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process. The change management would involve generating a request, risk assessment,

authorization from an appropriate authority, implementation, testing and verification of the change done.

- Potential security weaknesses / breaches (for example, as a result of analysing user behaviour or patterns of network traffic) should be identified.

- There should be measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.

- Applications must not allow unauthorized entries to be updated in the database. Similarly, applications must not allow any modifications to be made after an entry is authorized. Any subsequent changes must be made only by reversing the original authorized entry and passing a fresh entry.

- Direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.

- Access to the database prompt must be restricted only to the database administrator.

- Robust input validation controls, processing and output controls have to be built into the application.

- There is a procedure in place to reduce the reliance on a few key individuals.

- Error / exception reports and logs are reviewed and any issues is remedied /addressed at the earliest.

- For all critical applications, either the source code is received from the vendor or a software escrow agreement is put in place with a third party to ensure source code availability in the event the vendor goes out of business. It is ensured that product updates and programme fixes are also included in the escrow agreement.

- In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign banks, there needs to be suitable controls like segregation of data and strict access controls based on 'need to know' and robust change controls. The Company should be in a position to adequately prove the same to the regulator. Regulator's access to such data/records and other relevant information should not be impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees or other persons.

- An application security review/testing, initially and during major changes, needs to be conducted using a combination of source code review, stress loading, exception testing and compliance review to identify insecure coding techniques and systems vulnerabilities to a reasonable extent.

- Critical application system logs/audit trails also need to be backed up as part of the application backup policy.

- Robust System Security Testing, in respect of critical e-banking systems, needs to incorporate, inter-alia, specifications relating to information leakage, business logic, authentication, authorization, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. These need to be carried out at least on annual basis.

7. KYC for the Existing Accounts

While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions in existing customers would be continuously monitored for any unusual pattern in the operation of the accounts. Further if an existing customer is KYC compliant and she desires to open another account, there shall be no need for any fresh customer due diligence exercise.

8. Applicability to branches

The above guidelines shall also apply to all the branches of the company located in India or the branches which may be located abroad. However, in case any local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank of India .

9.Suspicion of money laundering/terrorist financing

With a view to preventing the Company 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, the Company shall carry out full scale customer due diligence (CDD) before opening an account.

10. Filing of Suspicious Transaction Report (STR)

The Company should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. In the circumstances when the Company 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. An indicative list of suspicious activities / transactions is enclosed in Annexure 2.

11. Record Management

The following steps shall be taken for maintaining, preserving and reporting of customer account information, with reference to provisions of PML Act and Rules. The company shall:

(a) maintain all necessary records of transactions with the customer, for at least five years from the date of transaction;

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

(c) make available the identification records and transaction data to the competent authorities upon request;

(d) 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;

(g) maintain records of the identity and address of their customer, and records in respect of transactions in hard or soft format.

12. Obligations under International Agreements

Communications from International Agencies –

The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, they do not have any account appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(a) The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

(b) **The"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

13. Secrecy Obligations and Sharing of Information

(a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship with the customer.

(b) While considering the requests for data/information from Government and other agencies, the Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(c) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law

ii. Where there is a duty to the public to disclose,

iii. the interest of the company requires disclosure and

iv. Where the disclosure is made with the express or implied consent of the customer.

(d) The Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

14. Allotment of Unique Customer Identification Code (UCIC)

The Company shall allot a Unique Customer Identification Code (UCIC) while entering into new relationships with individual customers as also the existing customers.

The Company shall, at its option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

B. Prevention of Money Laundering Act (PMLA), 2002 - Obligations of the Companying terms of Rules notified thereunder

1. Appointment of Principal Officer

For the purpose of this policy and compliance of KYC/AML/CFT regulations, Mr. Vinay Pratap Singh, Operations Head shall act as Principal Officer and put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. For the purpose of this policy and the compliance of KYC/AML/CFT regulations the Risk Head or any other officer(s) duly authorized by CEO to be designated as 'Principal Officer' shall act as the Principal Officer of the company. The name, designation and address of the Principal Officer has been duly communicated to the Director, Financial Intelligence Unit – India (FIU-IND). As per the NBFC guidelines, the Principal Officer will be located at the corporate office and will be responsible for ensuring compliance, monitoring transaction, and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, other NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

2.Appointment of Designated Director

For the purpose of this policy and the compliance of KYC/AML/CFT regulations, Mr. Anup Kumar Singh, Managing Director shall be the Designated Director. The name, designation and address of the Designated Director has been duly communicated to the Director, Financial Intelligence Unit – India (FIU-IND).

If the Director-FIU, in the course of any inquiry, finds that a reporting entity or its designated director (Mr. Anup Kumar Singh)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.

In view of the above, the Company should nominate a Director on their Boards as "designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012.

3. Maintenance of records of transactions

The Company to have a system of maintaining proper record of transactions as mentioned below:

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

(ii) all series of cash transactions integrally connected to each other which have to be 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;

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

(iv) all suspicious transactions whether or not made in cash.

4. Information to be preserved

The Company has to maintain the following information in respect of transactions:

(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.

5. Maintenance and Preservation of records

The Company has to 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. The identification records and transaction data should be made available to the competent authorities upon request.

(i) The Company shall also maintain records for a period of five years from the date of cessation of transaction between the clients and the company.

(ii) The records pertaining to the identification of the customer and his 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, as indicated in the paragraph, would continue to be preserved for at least ten years after the business relationship is ended.

6. Reliance on third party due diligence

The company has presently not delegated the due diligence activity of KYC verification to any third party and the same is being undertaken by its own. However, in case in future the if the company delegates this activity to any third party, it shall ensure the following in this regard:

1) the company shall immediately obtain (not later than two days) necessary information of such client due diligence carried out by the third party;

2) the company shall undertake 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) the company before delegations shall ensure 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;**7. Reporting to Financial Intelligence Unit-India (FIU-IND)**

In terms of the PMLA rules, the Company is 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

The Company should 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 NBFCs 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 is 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 NBFC as a whole may be compiled by the Principal Officer of the NBFC 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.

The Company 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. NBFCs should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

In regard to CTR, the cut-off limit of Rupees ten lakh is applicable to integrally connected cash transactions also. It is clarified that:

a) For determining integrally connected cash transactions, the Company 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.

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

c) All cash transactions, where forged or counterfeit Indian currency notes have to be used as genuine and should be reported by the Principal Officer to FIU-IND immediately in the prescribed format.

While making STRs, the Company should be guided by the definition of 'suspicious transaction. The Company should make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction.

8. Assessment and Monitoring of Risk

The Government of India had constituted a National Money Laundering/Financing of Terror Risk Assessment Committee to assess money laundering and terror financing risks, a national AML/CFT strategy and institutional framework for AML/CFT in India. Assessment of risk of Money Laundering /Financing of Terrorism helps both the competent authorities and the regulated entities in taking necessary steps for combating ML/FT adopting a risk-based approach. This helps in judicious and efficient allocation of resources and makes the AML/CFT regime more robust. The Committee made recommendations regarding adoption of a risk-based approach, assessment of risk and putting in place a system which would use that assessment to take steps to effectively counter ML/FT. The recommendations of the Committee were accepted by the Government of India for implementation.

Accordingly, the Company takes appropriate steps to identify and assess their ML/FT risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels.

In order to have an effective implementation of KYC/AML/CFT measures, the Company shall put in place a system of periodic review of risk categorization of customers and updating of customer identification data in a time-bound manner.

C. Combating Financing of Terrorism (CFT)

In terms of PMLA Rules, suspicious transaction should include transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The Company 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.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks, European Unions as well as France and financial institutions (including NBFCs). The Company ensures to update the consolidated list of individuals and entities as circulated by Reserve Bank. The Company also ensures that before opening any new account the name/s of the proposed customer does not appear in the list. Further, the Company has put in place procedures to 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.

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking/financial channels. It would, therefore, be necessary that adequate screening mechanism is put in place by the Company as an integral part of its recruitment/hiring process of personnel.

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. The Company is 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.

The Company should take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. The Company 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. The Company should give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in these countries.

1. Monitoring

Ongoing monitoring is an essential element of effective KYC procedures. The Company 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. The Company applies enhanced due diligence measures on high risk customers.

The Company has to subject these 'high risk accounts' to intensified transaction monitoring. High risk associated with such accounts is taken into account by the Company to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-ND.

2. Operation of Bank Accounts and money mules

The guidelines covered under this policy for opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules."

3. Accounts of Politically Exposed Persons (PEPs)

Customer Due Diligence (CDD) measures to be made applicable to Politically Exposed Person (PEP) and their family members or close relatives. Before establishing any relationship with the PEPs sufficient information including information about the sources of funds, accounts of family members and close relatives shall be gathered and the identity of the person shall be verified before accepting the PEP as a customer. The decision for entering into any business relationship with a PEP, shall be taken at a senior level. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming ape, the Company 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 similar procedure shall be applicable in case of accounts of PEP who are resident outside India.

The instructions are also applicable to accounts where PEP is the ultimate beneficial owner. Further, in regard to PEP accounts, the Company has 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.

4. Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In such cases, the Company may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

5. Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc. The Company should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank’s management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent’s country may be of special relevance. Similarly, the Company should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards wishes to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO the Company while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

6. Shell Banks

The Company should refuse to enter into a correspondent relationship with a **"**shell bank**"** (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Banks should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

7. Maintenance of records of transactions

Though it will be unlikely in the Company's case, due to its focus on lower income families, the Company has to have a system of maintaining proper record of transactions prescribed under Rule 3, of the Prevention of Money-Laundering and value of transactions, the procedure and manner of maintaining and verification and maintenance of records of the identity of the clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, as mentioned below:

all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency; 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; 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; all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

8. Information to be preserved

As per the NBFC guidelines, the Company is to maintain the following information in respect of transactions referred to in Rule 3:

(i) the nature of the transactions; the amount of the transaction and the currency in which it was denominated;

(ii)the date on which the transaction was conducted;

(iii)and the parties to the transaction.

9. Maintenance and Preservation of records

The Company should have 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. The Company should maintain for at least Ten years (10 Years) from the date of cessation of transaction between the Company 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.

The Company has to ensure that records pertaining to the identification of the customer and her address as defined in the Annexure 1 is obtained before disbursing the loans and during the course of business relationship, are properly preserved for at least Ten years (10 Years) after the business relationship is ended. The identification records and transaction data will be made available to the competent authorities upon request.

10. Uploading of all KYC Data on CERSAI Platform

All registered entities (RE's) are required to upload all KYC documents obtained from clients of the company with the prescribed authority Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI).

The Company undertakes to register itself with the authority and start the KYC uploading process as mandated by the RBI.

11. Updation in KYC Policy of the Company

The above policy shall be governed by the directions of RBI or such other regulatory authorities and shall be subject to changes issued by these authorities from time to time.

The above policy has been approved in accordance with the applicable laws and rules pertaining to KYC/AML/CFT issued by the Reserve Bank of India from time to time. Any regulatory amendment, in relation to such guidelines/regulations shall have the effect of suo-motto amendment of the policy.

SONATA FINANCE PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC), ANTI MONEY LAUNDERING (AML) &

COMBATING FINANCING OF TERRORISM (CFT) POLICY

ANNEXURE – 1

Customer Identification Procedure
Features to be verified and documents that may be obtained from customers in addition to Aadhar

Features	Documents
Accounts of individuals Legal name and any other names used Correct permanent address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) copy of the Job Card issued by NREGA duly signed by the officer of State/ Central Government (vi) letter issued by UIDAI containing details of name, address and aadhar number of the applicant (vii) Identity card with applicants photograph, issued by Central/ State Government Departments, regulatory authorities, PSU/ commercial Banks (viii) Letter from a recognized public authority or public servant verifying the identity and residence of the applicant(ix) Utility bills which are not more than 2 months old (x) Bank account statement (xi) Municipal tax receipt (xii) Ration Card (xiii) Letter from employer (subject to satisfaction) (any one document which provides customer information to the satisfaction of the company will suffice)
Accounts of companies/NGO - Name of the - Principal place of business - Mailing address - Telephone/Fax Number	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlers, beneficiaries and signatories- Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill
Accounts of Proprietary Concerns - Name, Address and Activity of the 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. NBFCs/RNBCs 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.

ANNEXURE -2

An Indicative List of Suspicious Activities Transactions Involving Large Amounts of Cash

Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques,

Transactions that do not make Economic Sense.

Activities not consistent with the Customer's Business

Attempts to avoid Reporting/Record-keeping Requirements

(i) A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

(ii) Any individual or group that coerces/induces or attempts to coerce/induce the Company's employee not to file any reports or any other forms.

Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

(i) A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.

(ii) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

(iii) A customer who has no record of past or present employment but makes frequent large transactions.

(iv) Certain Company Employees arousing Suspicion

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.

(ii) Negligence of employees/wilful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name
- Sudden surge in activity level

//**//**//