c

SPANDANA SPHOORTY FINANCIAL LIMITED

KNOW YOUR CUSTOMER AND ANTI-MONEY LAUNDERING MEASURES

Date of Implementation: November 11, 2016
Date of Revision: May 22, 2021

Policy for 'Know Your Customer and Anti-Money Laundering measures'

INTRODUCTION:

Spandana Sphoorty Financial Limited (herein after referred to as "Company" or "SSFL") is registered as Non-Banking Financial Company with Reserve Bank of India (RBI) and classified as Loan Company based on its asset / income pattern. During the course of its operations, the Company will strictly adhere to various directions, guidelines, circulars, instructions etc. as may be stipulated by RBI from time to time.

In accordance with Master Direction issued by Reserve Bank of India vide DBR.AML.BC.No.81/14.01.001/2015-16 on Master Direction - Know Your Customer (KYC) Direction, 2016 dated 25th February, 2016 and subsequent updation as latest as 1st April 2021, all Non- Banking Financial Companies should adopt and follow Know Your Customer policy (KYC) and Anti Money Laundering Standards (AML).

SSFL policies should always be read in conjunction with RBI Guidelines, directives, circulars and instructions. The company will apply best industry practices so long as such practice does not conflict with or violate RBI Guidelines.

The Company shall obtain KYC documents from the customers as per Annexure 1 subject to compliance of KYC & Anti Money Laundering Standards (AML) mentioned hereunder.

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

i) A person or entity that maintains and/or has a business relationship with the Company;

ii) One on whose behalf such relationship is maintained (i.e. the beneficial owner);

iii) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and;

iv) Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company say a wire transfer or issue of a high value demand draft as a single transaction.

OBJECTIVE:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The Company had framed its KYC policy incorporating the following four key elements:

1. Customer Acceptance Policy
2. Customer Identification Procedures;
3. Monitoring of Transactions; and
4. Risk management.

1. CUSTOMER ACCEPTANCE POLICY (CAP):

The guidelines for Customer Acceptance Policy (CAP) for the company are given below:

(a) No account is opened in anonymous or fictitious/Benami name.

(b) No account is opened where the company is unable to apply appropriate Customer Due Diligence measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

(c) No transaction or account based relationship is undertaken without following the Customer Due Diligence procedure.

(d) The mandatory information is sought for KYC purpose while opening an account and during the periodic updation as and when required.

(e) Optional/additional information is obtained with the explicit consent of the customer after the account is opened.

(f) The Company shall apply the Customer Due Diligence (CDD) procedure at the Unique customer identification code (UCIC)level. Thus, if an existing KYC compliant customer of the company desires to open another account with the same company, there shall be no need for a fresh CDD exercise.

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

(i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

(j) Where Permanent Account Number (PAN) is obtained, the same is verified from the verification facility of the issuing authority.

(k) In place of obtaining an equivalent e-document from the customer, Spandana shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

2. CUSTOMER IDENTIFICATION PROCEDURE (CIP):

The policy approved by the Board of the Company clearly spells out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a business 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 his/ her identity by using reliable, independent source documents, data or information.

The Company shall obtain sufficient information necessary to establish to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant Guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to the Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). For customers that are natural persons, the Company will obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company will (i) verify the legal status of the legal person/ entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure-I for guidance of the Company.

The Company has framed its own internal guidelines based on their experience of dealing with such persons/entities, normal lender's prudence and the legal requirements as per established practices. The Company will 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. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in the Annexure-I. Documentation requirements and other information shall 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 Company of India from time to time.

Necessary checks wherever and to the extent possible, shall be conducted before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities.

The documents requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Official(s) in charge of the Policy are empowered to make

amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance.

Customer Identification Procedure is carried out at different stages i.e.

(a) Commencement of an account-based relationship with the customer.
(b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
(c) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
(d) The company shall ensure that account is not opened only by mere introduction.

No deviations or exemptions shall normally be permitted in the documents specified for account opening.

MONITORING OF TRANSACTIONS:

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity attached with the client.

RISK MANAGEMENT:

The Board of Directors of the Company had ensured that an effective KYC programme is put in place through establishing appropriate procedures and ensuring their effective implementation. It covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company may in consultation with their boards, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Company ensures that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard may be put up before the Audit Committee of the Board on quarterly intervals.

For Risk Management, the Company shall have a risk based approach which includes the following:

(a) Customers shall be categorised as low, medium and high risk category, based on the assessment and risk

perception of Spandana.

(b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements will 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.

SECTION 3 OF THE PREVENTION OF MONEY LAUNDERING (PML) ACT 2002 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 as untainted property shall be guilty of offence of money laundering".

All transactions of suspicious nature shall be reported. The Principal Officer of the Company shall ensure that such reporting system is in place and shall monitor receipt of the reports.

All transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority by the Principal Officer.

The necessary documents, information and records would be maintained and preserved for the period prescribed under AML Act would be maintained.

Money Laundering and Terrorist Financing Risk Assessment by the Company:

(a) The company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc.

The assessment process is in consideration with all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, The Company also takes cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor shares with the company from time to time.

(b) The risk assessment by the company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the company. Further, the periodicity of risk

assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, the risk assessment review shall be reviewed not later than annually.

(c) The outcome of the exercise will be placed to the Board and shall be made available to the regulatory authorities as and when required.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and the company has Board approved policies, controls and procedures in this regard. Further, The Company shall monitor the implementation of the controls and enhance them if necessary

Customer Due Diligence (CDD) Procedure in case of Individuals

For undertaking CDD, Spandana shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

The Aadhaar number where, he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act, 2016.

The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the company.

The company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the company.

An equivalent e-document of any OVD, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo.

Any OVD or proof of possession of Aadhaar number under clause "(ab) of the RBI master direction", where offline verification cannot be carried out; the Company shall carry out verification through digital KYC.

Provided that for a period not beyond such date as may be notified by the Government for a class of the company, instead of carrying out digital KYC, the company pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the company and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. The company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subject to periodic internal audit/inspection by the company and shall be available for supervisory review.

OTP based E-KYC

• Spandana will conduct Offline Verification of Aadhaar for identification.

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No.S.O. 3183(E) dated November 26, 2015.

(b) In terms of provision of Rule 9(1A) of PML Rules, the company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) The company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the operational guidelines of CERSAI, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' as the case may be. The templates may be revised from time to time as required by CERSAI.

(d)The companies other than SCBs were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.

(e) The company shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the Template released by CERSAI.

(f) Once KYC Identifier is generated by CKYCR, the company shall communicate to the same to individual/LE as the case may be.

(g) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

(h)The company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(i) Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to a company with an explicit consent to download records from CKYCR, then such company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

- There is a change in the information of the customer as existing in the records of CKYCR;
- The current address of the customer is required to be verified;
- The company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

Selling Third party products

The Company acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

(a) The identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

(b) Transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

(c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) Transactions involving rupees fifty thousand and above shall be undertaken only by debit to customers' account or against cheques; and obtaining and verifying the PAN given by the account-based as well as walk-in customers.

CUSTOMER EDUCATION:

Implementation of KYC procedures requires the Company to demand certain information from customers which may be of personal nature or which have 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 will prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC

programme. The front desk staffs needs to be specially trained to handle such situations while dealing with customers.

APPOINTMENT OF COMPLIANCE OFFICER/ PRINCIPAL OFFICER:

The Company shall appoint a senior management officer to be designated as Compliance Officer. Compliance Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. He / She shall maintain close liaison with enforcement agencies, banks and any other institutions which are involved in the fight against money laundering and combating financing of terrorism. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

COMPLIANCE OF KYC POLICY:

The Company shall ensure compliance with KYC Policy through:

i. Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
ii. Allocation of responsibility for effective implementation of policies and procedures.
iii. Independent evaluation of the compliance functions of REs' policies and procedures, including legal and regulatory requirements.
iv. (Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures. Submission of quarterly audit notes and compliance to the Audit Committee.
v. The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

IDENTIFICATION OF BENEFICIAL OWNER:

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps to verify his/her identity shall be undertaken keeping in view the following:

(a)Where the customer 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.
(b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Hiring and training employees

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

On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for field staff, compliance staff and staff dealing with new customers. The Branch staff shall be specially trained to handle issues arising from lack of customer education.

Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the company, regulation and related issues shall be ensured.

RECORD MANAGEMENT:

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information. The Company shall,

(a) Maintain all necessary records of transactions between the Company and the customer, both domestic and international, 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) 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);

(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

  (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.

(f) 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 referred to in Rule 3 in hard or soft format.

Annexure – I KYC DOCUMENTATION

Details	**KYC Documents**
Photograph	2 passport size photographs of applicant, preferably, along with spouse

	combined, The photograph should be signed across on the front. In case of single woman, only client's photograph should be affixed and cross signed/thumb impressed by the client.
Identify Proof	1. Aadhar card **(Optional - preferred)** 2. Voter's Identity Card **(Most preferred)** 3. Passport 4. PAN card 5. Driving License 6. Job Card issued by NREGA duly signed by an officer of the State Government 7. Identity card (subject to the Company's satisfaction) / Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company
Address proof	1. Aadhar card **(Optional - preferred)** 2. Voter's Identity Card **(Most preferred)** 3. Ration card 4. Driving License 5. Passport 6. Letter from any recognized public authority 7. Electricity bill 8. Telephone bill 9. Bank account statement 10. Letter from employer (subject to satisfaction of the Company) 11. A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority. Any one document which provides customer information to the satisfaction of the company will suffice

*****