

KYC/ ANTI-MONEY LAUNDERING POLICY

Table of Contents

1. Introduction and Legal Provisions	4
2. Objectives & Scope.....	5
3. Definitions	6
4. Roles & Responsibility	10
A. Operations Team.....	10
B. Compliance Team	10
C. Principal Officer:.....	10
D. Designated Director	10
5. Key Elements of Policy	11
A. Customer Acceptance Policy (CAP).....	11
B. Customer Identification Procedure (CIP).....	12
C. Risk Management.....	12
D. Ongoing Transaction Monitoring and Reporting	15
6. Prevention of Money Laundering Act, 2002 - Obligations of BCPL.....	20
7. General Guidelines	23
8. Review & Deviation from Policy.....	24
9. Appendix.....	25
10. Annexures	26

Regulatory Reference:

- RBI/DBR/2015-16/18 Master Direction DBR. AML. BC. No. 81/14.01.001/2015-16 Know Your Customer (KYC) Direction, 2016 updated as amended thereafter.
- RBI/2015-16/108 DNBR Master Circular (PD) CC No. 051/03.10.119/2015-16 – 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards (AML) -'Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in terms of Rules notified thereunder' dated July 1, 2015 as amended thereafter.

Content Management

Document Control	
Title	Anti-Money Laundering Policy
DOC ID/ Number	BCPL/2024-19
Policy Owner	Compliance, Legal, Accounts & Business Team
Last date of update	21/02/2024
Version Number	2024_V1
Reviewed by	Whole Time Director
Approved by	Board of Directors

Version	Updates	Reviewed Date	Department / Team	Approved by
2024_V1	KYC policy	21/02/2024	Compliance	Board of Directors

This policy document will be reviewed and revised by the Compliance Team with the Whole-Time Directors consultation and with approval of board of directors in response to changed circumstances and in any event, at intervals of not more than 12 months or shorter review periods as may be stipulated by the Board.

1. Introduction and Legal Provisions

Blacksoil Capital Private limited (herein referred to as “BCPL” or “the Company”) is a Systemically Important, Non-Deposit taking, Non-Banking Finance Company (NBFC-ND-SI) registered with RBI.

BCPL strategically focuses on new opportunities to foster growth and sustainability. Apart from providing alternative credit to Growth Companies (GC), BCPL lends two more segments, namely, Financial Institutions (FI) and Supply Chain Financing (SCF), to provide alternative credit.

Blacksoil Capital Private Limited (herein after “BCPL” or “the Company”) has a policy to prevent Money Laundering practices within the organization. This KYC/Anti-Money Laundering (AML) Policy (the Policy) has been prepared in accordance with 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering & Prevention of Money Laundering Act, 2002 (PMLA Act). Compliance with these standards by the NBFCs in the country have become necessary for international financial relationships. The Department of Banking Operations and Development of Reserve Bank had issued detailed guidelines to the NBFCs based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary. All NBFCs were, therefore, advised to adopt the same with suitable modifications depending on the activity undertaken by them and ensure that a proper policy framework on ‘Know Your Customer’ and Anti-Money Laundering measures is formulated and put in place with the approval of the Board. NBFCs were advised to ensure that they are fully compliant with the instructions.

This policy covers the existing RBI / FIU guidelines relating to KYC/AML and any subsequent guidelines from the date of the Policy on KYC/AML will be implemented immediately, with subsequent ratification by the Board. Extant regulations will at any point in time override this Policy.

2. Objectives & Scope

Preamble: The Reserve Bank of India has been issuing guidelines in regard to the Know Your Customer (KYC) standards which need to be followed by banks and NBFCs and the measures to be taken in regard to Anti Money Laundering (AML)/ Combating the Financing of Terrorism (CFT). NBFCs are required to put in place a comprehensive policy framework, duly approved by the Board of Directors or competent authority authorized by the Board of Directors, in this regard. This policy document has been prepared in line with the RBI guidelines.

The objective of having a KYC / Anti- Money Laundering Policy & procedures is to prevent the Company from being used as a conduit, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures also enable the Company to know/understand its customers, to make its financial dealings better and manage the related risks prudently. Such procedures shall include incorporating the following four key elements with a view to: -

- i. lay down explicit criteria for acceptance of customers,
- ii. put in place an effective system and procedure for customer identification of the bona-fide individuals/non-individuals for opening of customer account,
- iii. implement a system to conduct customer due diligence (CDD) based on the risk factor associated with each customer and effective implementation of procedures to help control and mitigate the related risk,
- iv. monitor transactions of a suspicious nature and report the same to the Financial Intelligence Unit- India (FIU- IND), verification and maintenance of records of transactions of customers in accordance with PMLA and the Rules made thereunder.

This policy is applicable to all our offices and is to be read in conjunction with related operational guidelines issued by RBI from time to time. It is crucial that all those concerned fully understand the rationale behind AML directives, obligations and requirements, implement them consistently and are sensitive to the risks of the system being misused by unscrupulous elements therefore all the employees dealing with customers should have access of this policy.

The Company shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this policy to conform to the standards so prescribed. This policy is applicable across all branches / business segments of the company, and its financial subsidiaries as well as all the persons authorised by the Company including agents / intermediaries, or brokers on behalf of the NBFC. The Policy is to be read in conjunction with related operational guidelines issued from time to time and necessarily read with reference to the changes / modifications as advised by RBI from time to time. This policy shall be applicable to all verticals/products of the Company whether existing or rolled out in future.

BCPL 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 the Company's policies and procedures, including legal and regulatory requirements.
- iv. Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
- v. Submission of quarterly audit notes and compliance to the Audit Committee.

BCPL shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

3. Definitions

1.1. Customer

- a. For the purpose of KYC Norms, a 'Customer' is defined as a person defined under the KYC policy of the RBI and any amendment from time to time by the RBI which are at present as follows.

A Customer means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

- b. A "Person" shall have the meaning as defined under KYC policy of RBI (and any amendment from time to time by RBI) which at present is as follows:

'Person' shall include:

- a. an Individual;
- b. a Hindu Undivided Family;
- c. a Company;
- d. a Trust
- e. a Firm;
- f. an association of persons or a body of individuals, whether incorporated or not;
- g. every artificial juridical person, not falling within any one of the above person (a to f);
- h. any agency, office or branch owned or controlled by any one of the above persons (a to f)

1.2. Designated Director

"Designated Director" means a person designated by the Company to ensure overall compliance with

the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

- a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors
- Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

1.3. Principal Officer

"Principal Officer" means an officer at the management level nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

1.4. Money laundering

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 or crime and projecting it as untainted property shall be guilty of offence of money laundering".

1.5. Officially valid document (OVD)

"Officially Valid Document" (OVD) means the passport, the Permanent Account Number (PAN) Card, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name and address.

Provided that,

- a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

- b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof 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;
- c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

1.6. Central KYC Records Registry (CKYCR)

“CKYCR” means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

1.7. Digital KYC

“Digital KYC” means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the RE as per the provisions contained in the Act.

1.8. Digital Signature

“Digital Signature” shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

1.9. Equivalent e-document

“Equivalent e-document” means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital

Locker Facilities) Rules, 2016

1.10. **“Know Your Client (KYC) Identifier**

“Know Your Client (KYC) Identifier” means the unique number or code assigned to a customer by the Central KYC Records Registry.

1.11. **“Video based Customer Identification Process (V-CIP)”**

an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

1.12. **“Group”**

The term “group” shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).

1.13. **“Person”**

“Person” has the same meaning assigned in the PML Act and includes:

- a. an individual,
- b. a Hindu undivided family,
- c. a company,
- d. a firm,
- e. an association of persons or a body of individuals, whether incorporated or not,
- f. every artificial juridical person, not falling within any one of the above persons (a to e), and
- g. any agency, office or branch owned or controlled by any of the above persons (a to f).

1.14. “Beneficial Owner (BO)”

A list of persons who are to be considered as such BOs in relation to a customer is given below:

Type of Customer	Persons to be considered Beneficial Owners (BOs)
Public / Private Limited Companies (a)	<ul style="list-style-type: none"> • Natural person whether acting alone or together or through one or more juridical person, has/have controlling ownership interest. “Controlling ownership interest” means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company. • Natural person whether acting alone or together or through one or more juridical person who exercises control through other means. “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.
Partnership Firm (b)	<ul style="list-style-type: none"> • Natural person whether acting alone or together or through one or more juridical person, has/have ownership of/ entitlement to more than 10% of capital / profits of the partnership or who exercises control through other means. “control” shall include the right to control the management or policy decision.
Trusts/Foundations (C)	<ul style="list-style-type: none"> • Trustees/Author of Trust • Beneficiaries of the Trust with 10% 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.
Unincorporated association or body of individuals (d)	<ul style="list-style-type: none"> • Natural person whether acting alone or together or through one or more juridical person, has/have ownership of/ entitlement to more than 15% of the property or capital or profits of the unincorporated association or body of individuals • Term ‘body of individuals’ includes societies.

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

4. Roles & Responsibility

A. Business Team:

The following shall be the responsibilities:

- Collection & Procure of complete set of documents from the customer at the time of on boarding.
- Perform additional check of potential customers as per policy.
- Monitoring of day to day transactions in order to identify unusual/suspicious transactions.
- Support legal & compliance team for Investigation of suspicious transaction.
- Adherence to this policy with respect to customer on boarding, periodical review and transactions monitoring.

B. Compliance Team:

The following shall be the responsibilities:

- Review & Reporting the exception while onboarding the customer and share with senior business team for approval.
- Investigation of suspicious transactions reported and consult business team on potential suspicious transactions.
- Discuss and submit the details to Principal Officer (PO) about suspicious transactions and results of investigation.
- Adherence to this policy with respect to periodic compliance as applicable.

C. Principal Officer:

The following shall be the responsibilities:

- Overseeing and ensuring overall compliance including sharing and reporting information with regulatory guidelines on KYC/AML/TF/CFT issued from time to time.
- Ensuring overall compliance with obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time.
- The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
- Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

D. Designated Director:

- To ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.
- The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
- Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
- In no case, the Principal Officer shall be nominated as the 'Designated Director'

5. Key Elements of Policy

As per RBI Master circular / directions each registered intermediary shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia incorporating the following four key elements:

- A. Policy for acceptance of customers
- B. Procedure for identification of customers
- C. Risk Management
- D. Transaction monitoring

A. Customer Acceptance Policy (CAP)

Following norms and procedures will be followed by the Company in relation to its customers who approach the Company for availing financial facilities. While taking decision to grant any one or more facilities to customers as well as during the continuation of any loan account of the customer, the following norms will be adhered to by the Company:

1. Customers who are acceptable to BCPL as per the Risk categorization should fulfill all criteria related to submission of OVDs and more specifically stated under the Customer Identification Procedure in the table set out separately.
2. No loan account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account i.e. Benami Account. The Company shall insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.
3. Circumstances, in which a customer is permitted to act on behalf of another person /entity, shall be clearly spelt out in conformity with the established law and practices, as there could be occasions when an account is operated by a mandate holder or where an account may be opened by intermediary in a fiduciary capacity.
4. The Company shall not open any account or give / sanction any loan or close an existing account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:
 - The Company is unable to verify the identity of the customer and /or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The BCPL may also consider closing an existing customer account under similar circumstances.
 - The customer without any valid or convincing reasons refuses to provide documents to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity
 - Information furnished by the customer does not originate from the reliable sources or appears to be doubtful due to lack of supporting evidence.
 - Identity of the customer, directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.
5. Subject to the above-mentioned norms and caution, at the same time all the

employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

6. The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established.
7. Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.
8. The Risk Team shall, at the time of approving a financial transaction/activity, or executing any transaction, verify the record of identity, signature proof and proof of current address or addresses including permanent address of the customer. For co-lending loans, this shall be verified by the NBFC partner. The Company shall however maintain a repository of KYC documents of borrowers under the co-lending programme as well.

B. Customer Identification Procedure (CIP)

Customer identification means undertaking customer due diligence measures while commencing a customer account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of the OVDs. The identity of the customers would be verified by using reliable, independent source document, data or information.

BCPL shall obtain sufficient information to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the relationship. BCPL shall identify the beneficial owner(s) and take all reasonable steps as per guidelines to verify his identity.

The Customer Identification Procedures would be carried out at the following stages:

- While establishing a business relationship;
- While 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.

BCPL may seek 'mandatory' information required for KYC purpose which the customer is obliged to give while opening a customer account or during periodic updation. Other 'optional' customer details/additional information, if required may be obtained separately after the customer account is opened, only with the explicit consent of the customer.

The detailed procedure and documentations required for each type of customer for due diligence and identification is provided in the Annexure-1 hereto.

C. Risk Management

The level of Money Laundering (ML) risks of a Customer relationship will be determined on the basis of type of the customer and nature of business & type of product / service availed by the customer. For acceptance and identification, all the Customers will be categorized as per risk strategy. These parameters will be defined by RMC (Risk Management Committee) and reviewed periodically. The Broad principles may be laid down by the REs for risk-

categorization of customers.

Risk categorization of the Customers

Each Customer is classified into a Risk Category as per the Risk Strategy evolved by the Company. Various parameters may be considered to arrive at such Risk Category including

- Customer identity, the background of the customer,
- the nature of business of the customer,
- the information and location of business of the customer,
- Geographical risk covering customers as well as transactions,
- type of products/services offered,
- delivery channel used for delivery of products/services,
- types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions etc.,
- the locations from where majority of customer's business,
- financial / social standing of the customer,
- mode of payments
- amount involved in the financial transaction etc.

The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Risk Strategy

- A. The Company shall categorize its customers based on the risk perceived by the Company. The levels of categorization would be Low Risk, Medium Risk and High Risk. The risk categorization would be a function of the industry the borrower operates in, the geography in which the borrower operates, the shareholding pattern of the entity etc.
- B. The profile of new customers will be prepared on risk categorization basis. Such profile will contain the following information about the new customers:
 - Customer's Identity
 - Social/Legal and financial status of the customer
 - Nature of the business activity
 - Information about the business of the customer's clients and their locations
- C. There will be level-wise categorization of customers i.e. Level-I, Level-II and Level-III. Such levels will be decided based on risk element involved in each case which will be determined by considering the following information submitted by the customer:
 - Nature of business of the Customer and of his Clients
 - Workplace of Customers and of his Clients
 - Country of Origin
 - Source of funds
 - Volume of business six-monthly / annual turn-over
 - Social/Legal and financial status
 - Quantum and tenure of facility applied for and proposed schedule for repayment of

loan

- D. Information to be collected from the customers will vary according to categorization of customer from the point of view of risk perceived. However, while preparing customer profile the Company shall seek only such information from the customer which is relevant to the risk category and is not intrusive to the customer. Any other information from the customer should be sought separately with his/her consent and after opening the account.
- E. For risk categorization, individual (other than High Net Worth) and entities whose sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile, may be categorized as low risk or Level-I category. Normally Level-I customers would be
- Well governed corporates
 - Salaried employees having definite and well-defined salary structure,
 - Employees of Government Departments or Government owned companies,
 - Statutory bodies,
 - Self-employed individuals, however, with regular income and good credit behavior
- F. Cases where the Company is likely to incur higher than average risk will be categorized as medium or high-risk customers and will be placed in medium or high-risk category i.e. Level-II or Level-III category. While placing the customers in the above categories, the Company will give due consideration to the following aspects:
- Customer's background,
 - Country of his origin,
 - Nature and location of his business activities,
 - Sources of funds and profile of customer's clients etc.

In such cases, the Company will apply higher due diligence measures keeping in view the risk level.

- G. Special care and diligence will be taken and exercised in respect of those customers who happen to be high profile and/or Politically Exposed Persons ("PEP") or Special Category Customers ("SCC") within or outside country. Such persons will include:
- Foreign Delegates or those working in Foreign High commissions or Embassies,
 - Head of states/Governments,
 - Senior Politicians,
 - Senior Government or Judicial Officers,
 - Senior Military Officers,
 - Senior Executives of State-Owned Corporations and
 - Officials of important political party officials.

About the accounts of PEPs and SCC's, in the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP or SCC, the Company shall obtain Credit Committee approval in such cases to continue the business relationship with such person and

undertake enhanced monitoring.

- H. The extent of due diligence requirement will vary from case to case as the same will depend upon risk perceived by the Company while granting credit facilities to customers.
- I. Cases in which the risk level is higher will require intensive due diligence exercise. Such cases will include those where the sources of funds to be used for business operations or sources to repay the loan to the Company are not clearly disclosed or cannot be ascertained from the financial statements submitted by the customer to the Company. Besides above, some of such customers in whose cases the Company will require higher due diligence measures, especially those for whom the source of funds is not clear, are mentioned below:
- NRI Customers
 - Trusts (except trusts appropriately set up under a specific regulation)
 - Societies
 - Charitable Institutions
 - NGOs and other organizations receiving donations from within or outside the country
 - Partnership firms with sleeping partners
 - Family owned companies
 - Persons with dubious or notorious reputation as per the information available from different sources like media, newspapers etc
 - Companies having close family shareholding or beneficial ownership
 - Politically exposed persons (PEPs) of foreign origin means individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, Senior Politicians, Senior Government, important political officials
 - High net worth individuals
 - Non-face to face customers

Please note that in addition to the above steps, following additional check needs to be considered by Risk team and verified by the Compliance team while categorizing the customer in various risk category:

- **Credit Score Check** - To ascertain the creditability of the borrower (including Promoter/ Director/ Partners/ Karta) the team checks the CIBIL (Credit Information Bureau (India) Ltd) score of the borrower. The indicative minimum CIBIL score of the borrower (with a credit history) should not be less than 650. If CIBIL score anything between 550 to 650, Risk team / Credit team shall take specific approval of the board. However, in exceptional situations where there is no credit history or limited credit history of the borrower is available with CIBIL, we give emphasis on various other factors to check the

credit worthiness of borrowers like by analyzing the ageing report of debtors of the borrower and bank references of the borrower.

- **Credit Rating Check** – To predict the ability of the borrower to pay back the debt obligation and implicit forecast of the likelihood of the borrower default credit rating is checked for all corporate borrowers.
- **ROC Check** - All the borrowers are verified with the ROC which maintains a master database of all the registered companies and their compliances so as to ascertain genuineness of the details provided by corporate borrower.
- **Banned List Check** - All borrowers are screened through the banned list issued by the RBI & SEBI, Stock Exchange, FATF & UNSC database of regulatory actions against various entities available at respective websites of the regulators.
- **Arbitration Check**- Screening of the cases filed for arbitration with the stock exchanges available at the BSE/NSE website.
- **Willful Defaulter Check**- Any promoter/individual will be checked to ascertain if he or she has been declared as a willful defaulter.
- **Google Check**- A generic google check of the borrower will be completed for any negative news, legal checks and past history of defaults.
- **Watch out Investors Check** – To identify companies, intermediaries and individuals who have been indicted for an economic default or have been non-compliant of laws/guidelines.

D. Ongoing Transaction Monitoring and Reporting

Ongoing monitoring is an essential element of effective KYC procedures. The concerned team 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. The ongoing due diligence is based on the following principles & other principal as defined internally:

- a. The extent of monitoring will depend on the risk category of the customer account. High risk customer has to be subjected to more intensified monitoring.
- b. Examples of types of transactions:
 - i. Large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
 - ii. Transactions which exceed the thresholds prescribed for specific categories of customer accounts.
 - iii. Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer and when cash transactions of Rs.10 lakhs and above are undertaken, the Company will keep proper record of all such cash transactions in a separate register maintained at its office.
 - iv. High customer account turnover inconsistent with the size of the balance maintained.

BCPL shall put in place a system of periodical review of risk categorization of customers and the need for applying enhanced due diligence measures. Such review of risk categorization of customers should be carried out at a periodicity of **not less than once in six months**. The Risk & Business team shall conduct periodic due diligence and scrutiny of customer's transaction to ensure that

transactions are being conducted in knowledge and through the customer's bank account.

DUE DILIGENCE OF BUSINESS PARTNERS

The following due diligence must also be performed on prospective Business Partners.

A. Verify Identity:

- Obtain and file legible copies of corporate formation and registration documents or public company prospectuses and government filings.
- PAN card of the Directors etc.

- Wherever possible (in the case of privately-owned entities), arrange for recommendation from legal counsel to the company.

- Wherever possible (in the case of privately-owned entities), obtain from appropriate government entity confirmation of due incorporation and existence of the corporation.

B. Verify Source of Income:

- Research for the Company details in available news or business databases and obtain all corporate earnings information available.

DUE DILIGENCE ON EMPLOYEES

The Company shall perform the following Due Diligence on Prospective Employees prior to their date of joining

A. Verify Identity:

- a. Obtain originals of and file legible copies of identification documents that contain photographs of the individual. Acceptable examples include:
 - i. Passports (obtain all nationalities an individual may have)
 - ii. PAN card
 - iii. Driver's license
 - iv. UID or Physical Aadhaar card/letter or e-Aadhaar letter

B. Verify Domicile of Residence

- a. Example: Obtain copies of utility bill receipts or other form of objective verification of Residence, UID or Physical Aadhaar card/letter or e-Aadhaar letter (if the address provided by the customer is the same on the document submitted for identity proof)

C. Verify the previous year's Employment Record:

- a. Obtain and call the previous employer to check the credentials of the prospective employee
- b. Check and verify the address of employee

D. Check References:

- a. Obtain 2 or more professional employment references from the prospective employee.
- b. The prospective manager of the employee, or, the Human Resources department, must personally converse with the prospect's references. The Company shall maintain files for each employee hired together with copies of all data obtained. These files may be maintained in electronic or physical form and should be accessible quickly when needed.

The Company shall maintain files on each Business Partner with copies of all data obtained and memorialize in writing all the verification efforts. These files may be maintained electronically and

should be accessible quickly when needed.

Customer Education:

Implementation of KYC procedures requires the Company to demand certain information from customers which may be of a 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 will prepare specific literature/ pamphlets etc. so as to educate the customer on the objectives of the KYC programme. The business team needs to be specially trained to handle such situations while dealing with customers.

Introduction of New Technologies

The Company will assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and preexisting products.

Further, The Company shall ensure:

- (a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- (b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc

DUE DILIGENCE FOR BANKS (LENDERS)

Being an SI-ND-NBFC, BCPL shall comply all the regulations stated specifically for Systemically important Non-Deposit taking NBFC while availing the facility from the lender. Self-Certified KYC's of authorized signatories shall be provided to Bankers. The loan documents shall be executed by the person authorized

by the board. Monitoring of the covenants mentioned in the loan documents executed with respect to the facility availed from bankers shall be done on ongoing basis. In case of breach of any covenants, the same shall be immediately informed to the bankers and the necessary steps shall be taken to make it good. Money borrowed shall be utilized for the purpose it is sanctioned. Overseeing and ensuring overall compliances from time to time

DUE DILIGENCE FOR VENDOR

- Self-Certified KYC's of authorized signatories shall be procured from the Vendors.
- Vendor registration form (VRF) shall be filled by the upcoming vendor and adequate documents shall be procured as enumerated in the VRF.
- Up-dation of KYCs shall be done a yearly basis.

UPDATION/PERIODIC UPDATION OF KYC :

The updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers. For 'low risk', customers in case there is no change in status with respect to their identities and

addresses, a self-certification by the customer to that effect should suffice in such cases. A certified copy of the document (proof of address) could be sent by mail / post, etc. Policy in this regard shall be documented as part of the Company's internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.

a) Individuals:

- i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter, etc.
- ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

Further, the Company, at their option, may obtain a copy of OVD or deemed OVD, as defined in Section 3(a)(xiv), or the equivalent e-documents thereof, as defined in Section 3(a)(x), for the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the Company in their internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.

- iii. **Accounts of customers, who were minor at the time of opening account, on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Company. Wherever required, the Company may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major.
- iv. **Aadhaar OTP based e-KYC in non-face to face mode** may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Customers other than individuals:

- i. **No change in KYC information:** In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter from an official authorized by the LE in this regard, board resolution, etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- ii. **Change in KYC information:** In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer.

C) Additional measures: In addition to the above, the Company shall ensure that,

- i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- ii. Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records /database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- iv. In order to ensure customer convenience, the Company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.
- v. The Company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.

Enhanced and Simplified Due Diligence Procedure

Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17): Nonface-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such nonface-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and nondigital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by REs for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

- a) In case the Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. The Company shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
- c) Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- d) The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

6. Prevention of Money Laundering Act, 2002 - Obligations of BCPL

Principal Officer

BCPL shall appoint a senior management officer to be designated as Principal Officer. The role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time.

With a view to enable the Principal Officer to discharge his responsibilities, the Principal Officer and other appropriate employee have timely access to customer identification data and other CDD information, transaction records and other relevant information. Name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

1. To ensure the monitoring and reporting of all transactions and sharing of information as required under Rule 7 of the Prevention of Money Laundering (Maintenance of Records etc.) 2005.
2. Principal Officer for KYC will act independently and report directly to the concerned Director to the Board of Directors.
3. Principal Officer shall be located at the head/corporate office of NBFC.
4. Principal Officer shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.
5. He/ She will maintain close liaison with enforcement agencies, NBFC and any other institution which are involved in the fight against money laundering and combating financing of terrorism.
6. Further, the role and responsibilities of the Principal Officer shall include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.
7. The Principal Officer will also be responsible for timely submission of CTR, STR to FIU-IND.
8. With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information

Designated Director

BCPL shall designate a designated director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board. Name, designation and address of the Designated Director shall be communicated to the FIU-IND. In no case, the Principal Officer shall be nominated as the Designated Director.

Maintenance of records of transactions

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

- All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.

- Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all customers of the same customer' should be considered.
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions.
- All suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

BCPL shall maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as

to permit reconstruction of individual transaction, including the following information:

- the nature of the transactions.
- the amount of the transaction and the currency in which it was denominated.
- the date on which the transaction was conducted.
- the parties to the transaction.

Preservation of records

BCPL shall take appropriate steps to evolve a system for proper maintenance and preservation of customer information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

- BCPL shall maintain for at least five years from the date of transaction between the Company and the customer, all necessary records of transactions which will permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.
- BCPL would ensure that records pertaining to the identification of the customers and their address obtained while opening the customer account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule.
- Special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Reliance on third party due diligence

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

- Immediately obtains necessary information of such customer due diligence carried out by the third party.
- Takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from

the third party upon request without delay.

- To satisfy that such third party is regulated, supervised or monitored for, and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- The third party is not based in a country or jurisdiction assessed as high risk.
- BCPL is ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable.

Transactions Monitoring

“Suspicious transaction” means a “transaction” as defined below, including an attempted transaction, whether made in cash, which, to a person acting in good faith:

- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to not have economic rationale or bona-fide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Examples of suspicious transactions are indicated as under:

- ❖ Identity of customer
 - False identification documents
 - Identification documents which could not be verified within reasonable time
 - Non-face to face customer
 - Doubt over the real beneficiary of the customer
 - Customer accounts opened with names very close to other established business entities
- ❖ Background of customer
 - Suspicious background or links with known criminals
 - Large number of customers having a common customer account holder, introducer or authorized signatory with no rationale
- ❖ Transactions
 - Value just under the reporting threshold amount in an apparent attempt to avoid reporting
 - Value inconsistent with the customer’s apparent financial standing
 - Transactions Involving Large Amounts of Cash
 - Transactions that do not make Economic Sense
 - Activities not consistent with the Customer's Business
 - Large Cash Transactions
 - Unexplained transfers between multiple customer accounts with no rationale

The Compliance team shall ensure updation of such list from time to time based on the understanding of the market scenarios and customer trading patterns.

The Risk & Business team is responsible to monitor the transactions on a day to day basis and in case of any unusual transactions noted or identified the same shall be reported to the Compliance team for further investigation.

The Principal Officer shall put in place a transaction alert which will provide proactive signals on suspicious transactions.

Reporting of Suspicious Transactions

In terms of the PMLA rules, principal officer shall report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND), presently, at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021

Reporting of transactions should be carried out in such format and such manner, as prescribed by FIU and other Regulatory Authorities from time to time.

The Principal Officer is responsible for timely submission of CTR/STR to FIU-IND and the STR is to be submitted 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 will record his reasons for treating any transaction or a series of transactions as suspicious. It will be ensured that there is no undue delay in arriving at such a conclusion.

7. General Guidelines

Master Circular – 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards (AML) - Prevention of Money Laundering Act, 2002 has as specified certain general guidelines. BCPL will ensure that following general guidelines wherever applicable will be adhered by the Company:

- i. CDD Procedure and sharing KYC information with Central KYC Records**
BCPL would upload and fetch the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.
- ii. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)**
Under FATCA and CRS, BCPL would adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F.
- iii. Unique Customer Identification Code (UCIC)**
BCPL would allot UCIC while entering new relationships with individual customers as also the existing customers. A Unique Customer Identification Code (UCIC) will help the Company to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable to have a better approach to risk profiling of customers.
- iv. Confidentiality of customer information:**
Information collected from customers for the purpose of opening of customer account is to be treated as confidential and details thereof should not be divulged for the purpose of cross selling, etc. Any other information that is sought from the customer should be called for separately only after the customer account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It should be indicated clearly to the customer that providing such information is optional.
- v. Sensitizing customers:**
Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. BCPL should, therefore, prepare specific literature/pamphlets, etc. to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited.
- vi. Employee training:**
BCPL shall have an ongoing employee training program so that the members of employee are adequately trained in AML/CFT policy. The focus of the training should be different

for frontline employees like compliance employees and employees dealing with new customers. The front desk employee needs to be specially trained to handle issues arising from lack of customer education. Awareness would be created in terms of AML standards and its measures with the help of training/media which will be towards ensuring that BCPL is not used intentionally or unintentionally for the purpose of money laundering.

vii. Employees Hiring

BCPL shall have an adequate screening mechanism to ensure high standards as an integral part of its personnel recruitment/hiring process shall be put in place. The Company shall endeavor to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff. It would identify the key positions within the organization structure having regard to the risk of money laundering and terrorist financing and the size of its business and ensure the employees taking up such key positions are suitable and competent to perform their duties. Accordingly, all employees of BCPL having the designation of vice-president and above and dealing with customers or with their funds and securities will be treated as "key positions". HR will ensure that employees taking up such key positions are suitable and competent to perform their duties.

viii. Closure of Customer accounts/Termination of Financing/Business Relationship:

Where BCPL is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-operation by the customer, the Company would terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision would be taken with the approval of whole-time director or principal officer.

8. Review & Deviation from Policy

Review of Policy

The Directors of BCPL will be authorized to amend/modify the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments time to time.

Circulation of Policy and Failure to Comply

The employee will be made aware of the Know Your Customer policies and Anti Money-Laundering Measures adopted by BCPL and they will be kept informed of the changes/modifications therein. It would be ensured that the employees religiously follow the Know Your Customer policies and Anti Money- Laundering Measures adopted by BCPL.

Violation of this Policy by employees will be referred to the BCPL Human Resource Department for disciplinary action and will be deemed to be misconduct under the BCPL HR Manual.

Deviation from Policy

Any request for deviation from this policy, which may become necessary due to practical difficulties in implementation or otherwise, would be referred to the BCPL Principal Officer. Thereupon, on case to case basis, Principal Officer can take final decision based on the facts of the case & considering the compliance requirements.

9. Appendix

Sr No	Abbreviation	Full Form
1	AML	Anti-Money Laundering
2	CDD	Customer Due Diligence
3	CEO	Chief Executive Officer
4	CIN	Corporate Identification Number
5	CTR	Cash Transaction Report
6	DIN	Director Identification Number
7	DOC	Document
8	FII	Foreign Institutional Investor
9	FIU	Financial Intelligence Unit
10	FT	Financing Terrorism
11	HR	Human Resource
12	IC	Investment Committee
13	IM	Investment Manager
14	KYC	Know Your Customer
15	LLP	Limited Liability Partnership
16	MD	Managing Director
17	ML	Money Laundering
18	OVD	Officially Valid Documents
19	PAN	Permanent Account Number
20	PMLA	Prevention of Money Laundering
21	POA	Proof of Address
22	POI	Proof of Identity
23	SLA	Service Level Agreement
24	STR	Suspicious Transactions Reporting
25	EDD	Enhanced Due Diligence
26	TF	Terrorist Financing
27	LE	Legal Entities

10. Annexures

Customer Identification Procedures (Documents that may be obtained from customer)

MANDATORY DOCUMENTS REQUIRED (For Individual &

Non- Individual) Annexure-01

For Individual	Documentary Requirements
Important Points:	<ul style="list-style-type: none"> i. In cases where the customer is CKYC complaint then obtain documents from the CKYC registry along with the KRA number. In cases the customer is not CKYC registered then the following documents should be obtained. ii. Self-attested copy of PAN card is mandatory for all customers. iii. Copies of all the documents submitted by the applicant should be self- attested and accompanied by originals for verification. iv. If any proof of identity or address is in a foreign language, then translation into English is required. v. In case of foreign national the copies of documents should be properly attested/apostille by entities authorized for attesting the documents.

For Non-Individuals	Documentary requirements
Documents to be submitted to the Company (Lenders)	<ul style="list-style-type: none"> i. RBI registration certificate ii. Certificate of Incorporation iii. Certified True copies of the Memorandum and Articles of Association iv. KYCs for the company v. Certified List of Shareholders/Promoters/Directors. vi. Photograph, POI, POA, PAN and DIN of directors & individual promoters holding control either directly or indirectly. vii. Beneficial ownership details viii. Last 3-month Bank Statement. ix. Authorised Signatories list with specimen signatures x. An officially valid document in respect of the person holding an attorney to transact on its behalf. xi. Latest financials of the customer of last 2 years

Details of the Principal Officer:

Principal Officer	Contact Number	Zone	Office Address	Landline Number	Email id
Ankur Banal	+91 982025433 5	All India	1203, Lodha Supremus, Senapati Bapat Marg, Lower Parel, Mumbai - 400013	022- 24812200	ankurbansal@blacksoil.co.in