BHANIX FINANCE AND INVESTMENT LIMITED

ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER POLICY

Adopted / Amendment Date by Board	Reviewed By	Approved By	Version No	Last Review Date
April 25, 2024	Head of Operations and Chief Compliance Officer (CCO)	Chief Executive Officer	2	21st April 2022

Table of Contents

1. BACKGROUND

Bhanix Finance Investment Limited (hereafter referred to as 'the BFIL'/ 'the Company') is a public limited company incorporated under the provisions of Companies Act, 1956 registered with Reserve Bank of India (RBI). In accordance with the Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023, the company is categorized as a Non-Banking Financial Company – Middle Layer.

In order to prevent NBFCs from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

Provisions of Prevention of Money Laundering Act, (PMLA) 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). The Reserve Bank of India (RBI) has issued Master Direction- Know Your Customer (KYC) Direction, 2016, dated 25th February 2016 and as amended from time to time applicable to all Non- Banking Financial Companies (NBFCs). In view of the same, the Board of Directors of BFIL has adopted this policy framework on AML – KYC measures in line with RBI guidelines. This policy is applicable to Bhanix Finance and Investment Limited and it's holding/ subsidiary companies.

2. OBJECTIVE, SCOPE AND APPLICATION OF THE POLICY

The KYC policy has been framed by the Company with the following objectives:

- To prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities;
- To enable the Company to know and understand its customers and their financial dealings better which will in turn help the Company to manage its risks prudently;
- To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
- To comply with applicable laws and regulatory guidelines;
- To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

3. DEFINITIONS

a. "**Act**" and "**Rules**" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

b. "**Aadhaar number**" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

c. "**Authentication**", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

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

Explanation- For the purpose of this sub-clause-

"Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

i. "Control" shall include the right to appoint a 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.

ii. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

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

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

iv. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

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.

e. **"Certified Copy"** - Obtaining a certified copy shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the RE as per the provisions contained in the Act.

f. **"Central KYC Records Registry"** (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.

g. **"Customer"** – means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.

h. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

i. **"Customer identification"** means undertaking the process of CDD.

j. **"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.

k. **"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 Company.

l. **"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).

m. **"Equivalent e-document"** means an electronic equivalent document, issued by the issuing authority 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.

n. "**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).

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

p. "**Non-face-to-face customers**" means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

q. "**Officially Valid Document (OVD)**" means the passport, 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 and letter issued by the National Population Register containing details of name and address. Provided that –

1. 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.

2. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -

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

b. Property or Municipal tax receipt;

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

d. 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 licence agreements with such employers allotting official accommodation;

3. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at '2' above.

4. 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.*

r. "**Offline Verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

s. "**On-going Due Diligence**" means regular monitoring of transactions in accounts to ensure that those are consistent with the Company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

t. "**Payable-through accounts**" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

u. "**Periodic Updation**" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

v. "**Politically Exposed Persons** (PEPs)" are individuals who are or have been entrusted with prominent public functions domestically or by a foreign country, e.g., Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

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

x. "**Suspicious transaction**" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith.

1. 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

2. Appears to be made in circumstances of unusual or unjustified complexity; or

3. Appears to not have economic rationale or bona-fide purpose; or

4. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

y. "**Unique Customer Identification Code (UCIC)**" shall mean a unique code provided to the customers by the Company while entering into an account-based relationship with the customer in order to maintain identification records.

z. "**Video-based Customer Identification Process (V-CIP)**": Video based Customer Identification Process (V- CIP) is an alternate method of customer identification with facial recognition and customer due diligence by authorized official of the Company 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.

4. KYC PROCESS

This KYC policy has the following four key elements:

a. Customer Acceptance Policy ("CAP") as set down under **Annexure 1**. The Customer Acceptance Policy shall enable the Company to treat all its customers at par and shall not allow discrimination against those who are financially or socially disadvantaged.

b. Customer Identification Procedures ("CIP") are as set down under **Annexure 2**.

c. Customer Due Diligence (CDD) Procedures: The features to be verified and documentary proof required from customers of each type and/or their Power of Attorney (POA) holder and/or their Beneficial Owners as set down under **Annexure 3 and 4**.

d. Risk Management - The Company shall have a risk-based approach as set down under **Annexure 5**. Customers shall be categorized as low, medium and high-risk categories, based on the assessment and risk perception. Risk categorization shall be broadly undertaken on the basis of parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc.

5. DESIGNATED DIRECTOR

The Company has appointed the 'Designated Director' duly nominated and appointed by its Board of Directors for the purpose of ensuring overall compliance by the Company under PMLA Act and its Rules. The Company will communicate the name, designation and address of the Designated Director to the FIU-IND. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI. The Designated Director of the Company shall be the person other than Principal Officer of the Company.

6. PRINCIPAL OFFICER

The Company has appointed the 'Principal Officer', who will be responsible for ensuring compliance under AML and KYC requirements under PMLA and rules framed thereunder, RBI requirements, CKYC/e-KYC and under such other requirements, monitoring transactions and sharing and reporting information as required under applicable law. The Company will communicate the name, designation and address of the Principal Officer to the FIU-IND. Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

7. COMPLIANCE WITH KYC POLICY

The Company shall ensure compliance with its KYC policy through:

- CEO, Head - Operations and Head - Compliance shall constitute the 'Senior Management', responsible for overseeing the effective implementation of KYC compliances.
- Operations Team shall be responsible for implementation of the policies and procedures.
- The Senior Management shall conduct independent evaluation of the KYC compliance functions of the company's policies and procedures, including legal and regulatory requirements.

- Effective Concurrent/ Internal audit system shall be in place to verify the compliance with KYC/AML policies and procedures.
- The aforesaid audit report shall be submitted by the Company to its Audit Committee.

8. ONGOING DUE DILIGENCE

BFIL shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds/wealth. For ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

9. PERIODIC UPDATION (RE-KYC)

The Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic 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 from the date of opening of the account / last KYC updation or whenever a new transaction is initiated by the borrower, whichever is later.
Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation by the Company.

a. Individual Customers:
    i. No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer shall be obtained through customer's email-id registered with the BFIL, customer's mobile number registered with the BFIL, ATMs, digital channels (such as online banking / internet banking, mobile application of BFIL), 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 BFIL, customer's mobile number registered with the BFIL, ATMs, digital channels (such as online banking / internet banking, mobile application of BFIL), 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, BFIL, at their option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

b. Customers other than individuals:
   i. No change in KYC information: In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration shall be obtained from the LE customer through its email id registered with the BFIL, ATMs, digital channels (such as online banking / internet banking, mobile application of BFIL), letter from an official authorized by the LE in this regard, board resolution etc. Further, BFIL 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, BFIL shall undertake the KYC process equivalent to that applicable for on boarding a new LE customer.

c. Additional measures: In addition to the above, BFIL shall ensure that –
   i. The KYC documents of the customer as per the current CDD standards are available with the Company. This is applicable even if there is no change in customer information but the documents available with the BFIL are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the BFIL has expired at the time of periodic updation of KYC, BFIL shall undertake the KYC process equivalent to that applicable for on boarding a new customer.
   ii. Customer's PAN details, if available with the BFIL, 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. BFIL shall adopt a risk-based approach with respect to periodic updation of KYC.
   v. BFIL shall advise the customers that to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the REs the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the Company's end.

In case of existing customers, BFIL shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60 of the customer. Provided that before temporarily ceasing operations for an account, BFIL shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, BFIL shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury,

illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring. Provided further that if a customer having an existing account-based relationship with a BFIL gives in writing to the BFIL that he does not want to submit his Permanent Account Number or equivalent e- document thereof or Form No.60, BFIL shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

- Periodical Review of Risk Categorisation:
    - A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place. Higher risk accounts shall be subjected to intensive monitoring.

- Enhanced Due Diligence
    - ***Accounts of non-face-to-face customers*** (other than Aadhaar OTP based E-KYC on-boarding): Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital 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 the Company:
        - 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. However, the facility shall be available only during the working hours and on a day which is not a public holiday of the Company. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP.
        - Customers with annual disbursed loan amount <INR 60,000 shall be treated as high- risk customers and no V-CIP shall be carried out for such customers. For customers with annual disbursed loan amount >= INR 60,000, V-CIP shall be carried out and no further due-diligence shall be needed for such accounts and they will be classified as low-risk customers (from KYC perspective as per Annexure 5 of this policy).
        - In order to prevent fraud, 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. In case of request of a change of mobile number from the customer, below steps to be followed:
        - The customer to initiate a formal request from the registered email id or letter to the Company for a change of mobile number, (efforts may be made to ensure that the new/updated mobile number is linked with Aadhaar).
        - On receipt of a formal request from the Customer, the Company to initiate Aadhaar-based OTP verification of mobile number.
        - Post successful verification of mobile number, the customers' details to be updated in the records of the Company.

- The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- The Company is in the business of digital lending through mobile based application 'CASHe'. Thus, for operational efficiency, first transaction in such accounts shall be a debit to the existing KYC-complied bank account of the customer (in the form of a penny-drop).

- Accounts of Politically Exposed Persons (PEPs)
  - BFIL shall have the option of establishing a relationship with PEPs provided that:
    - The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
    - Reasonable measures are taken by the Company for establishing the source of funds / wealth.
    - The approval to open an account for a PEP shall be obtained from the senior management.
    - All such accounts are subjected to enhanced monitoring on an on-going basis.
    - In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

10. RECORD MANAGEMENT

The Company shall take the following steps regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules.

- Maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction.
- 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.
- Make available swiftly the identification records and transaction data to the competent authorities upon request.
- 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).

Rule 3 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 lays down the following obligations for the maintenance of records:

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

- all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency.
- All transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency.
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.
- All suspicious transactions whether or not made in cash.
- all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.
- All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

- The records maintained shall contain the following information to permit the reconstruction of the individual transaction:
    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
- 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.
- Maintain a record of all the transactions above including identity and address of the customer in hard or soft format.

Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

11. REPORTING TRANSACTIONS

- If applicable, reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) shall be adhere to as per provisions of Income Tax Rules.
- The Principal Officer of the Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of rule 7 thereof. A copy of such information shall be retained by the Principal Officer for the purposes of official record.
- Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

- BFIL shall not put any restriction on operations in the accounts merely on the basis of the STR filed.
- The Company, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential.
- RBI has clarified that FINnet gateway portal has to be used for uploading of STR. FIU has enabled Web filing for uploading STR in both Account based Reporting Format (ARF) and Transaction based Reporting Format (TRF). Web filing involves data entry of details on an online web page for submitting reports to FIU-IND.
- The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).
- The Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.
- The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India as updated from time to time.

12. CASH TRANSACTIONS REPORTS (CTR)/ SUSPICIOUS TRANSACTION REPORTS (STR)

As required under RBI regulations, the Company shall ensure filing of all required Suspicious Transaction Report (STR) and Cash Transaction Report (CTR) to Financial Intelligence Unit – India (FIU-IND) within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

The Principal Officer should record his reasons for treating any transaction as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or other office. Such a report shall be made available to the competent authorities on request. Illustrative list of activities which would be construed as suspicious transactions is given in **Annexure 6**.

13. MONITORING OF TRANSACTIONS

On-going monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. The Company must pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The extent of monitoring shall be aligned with the risk category of the customer. Higher risk accounts shall be subjected to intense monitoring.
The following activities may form part of the monitoring function:

a. The account of the Customer after signing of the contract to be closely monitored for signs of any unusual transactions.
b. All Cash & suspicious transactions are required to be reported within the timelines given under the Prevention of Money Laundering Act ('PMLA'), 2002; the PML Rules 2005 framed thereunder; and the Foreign Regulation Act 2010.
c. High-risk accounts shall be subjected to intensified monitoring.
d. The Company should maintain a record of all transactions and take steps to preserve the same.

14. INTERNAL ML/ TF RISK ASSESSMENT

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, countries or geographic areas, products, services, transactions or delivery channels, etc

While assessing the ML/TF risk, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

The risk assessment by the Company should be properly documented. The risk assessment exercise should be reviewed at least annually. The outcome of the exercise shall be put up with the Risk Management Committee and should be available to competent authorities and self-regulating bodies.

Also, the Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and shall have Board approved policies, controls and procedures in this regard.

15. EMPLOYEE TRAINING

Periodic training programmes will be organized for employees to have adequate screening mechanism as an integral part of their personnel recruitment/hiring process.

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. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

An on-going employee training programme shall be put in place so that the employees are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education.

Proper staffing of the audit function with people adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured shall be put in place in AML procedures.

16. SHARING OF INFORMATION WITH CKYCR

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

Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to a RE, with an explicit consent to download records from CKYCR, then such RE 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 –

a. There is a change in the information of the customer as existing in the records of CKYCR.
b. The current address of the customer is required to be verified.
c. the RE 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.
d. The validity period of documents downloaded from CKYCR has lapsed

17. UNIQUE CUSTOMER IDENTIFCATION CODE (UCIC)

UCIC shall be allotted while entering into new relationships with the individual customers as also the existing individual customers.

18. INTRODUCTION OF NEW TECHNOLOGIES

The Company shall identify and assess the Money Laundering/Terrorist Financing (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 pre-existing 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.

19. CONFIDENTIALITY

Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
While considering the requests for data/information from Government and other agencies, REs shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions. The exceptions to the said rule shall be as under:

a. Where disclosure is under compulsion of law
b. Where there is a duty to the public to disclose
c. The interest of the Company requires disclosure and
d. Where the disclosure is made with the express or implied consent of the customer

20. REVIEW AND AMENDMENTS

The Company shall review the policy on an annual basis or at earlier intervals, if there any regulatory changes necessitating such interim reviews.

ANNEXURE 1

Customer Acceptance

- No account shall be opened by BFIL in anonymous or fictitious/benami names.
- Customer/ Authorised Signatory shall be a major (i.e., 18 years or above) and must not be incapacitated for entering into a contract as per Indian Contract Act.
- No account shall be opened where BFIL is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- No transaction or account-based relationship shall be undertaken without following the CDD procedures.
- Account shall not be opened if the mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is not specified.
- Information (not specified in the internal KYC policy of the Company) shall be obtained with the explicit consent of the customer.
- BFIL shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise.
- CDD Procedure will be followed for all the joint account holders, while opening a joint account
- Suitable system has been 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 indicated in Chapter IX of the KYC Master Directions.
- Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 02, 2021 and as amended from time to time.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, BFIL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

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.

ANNEXURE 2

Customer Identification Procedures

Customer identification means identifying the customer and verifying his / her / its identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain sufficient information such as PAN, Voter ID card / Passport / Officially Valid Documents, etc. necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Company will not insist on obtaining Aadhar except for those accounts intended to receive government subsidies /subvention or benefits under direct benefit transfer scheme of the Government. However, customer voluntarily producing Aadhar for the purpose of identification will be accepted by the company.

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, Company shall 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 shall

a. Verify the legal status of the legal person/ entity through proper and relevant documents.
b. 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.

Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. An indicative list of the nature and type of documents/information that may be relied upon for Customer Identification Procedure as given in **Annexure 4**.

The Company shall undertake identification of customers in the following cases:

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. As and when applicable, selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company shall, rely on Customer Due Diligence (CDD) done by a third party, subject to the following conditions:

Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

a. Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

b. The Company shall take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

c. The 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 Prevention of Money-Laundering Act.

d. The third party shall not be based in a country or jurisdiction assessed as high risk.

e. The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall rest with the Company.

ANNEXURE 3

CUSTOMER DUE DILIGENCE (CDD) PROCEDURE IN CASE OF INDIVIDUALS

For undertaking CDD, the Company 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:

a. The Aadhaar number where

   i. he/she is 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 (18 of 2016); or.

   ii. he/she decides to submit Aadhaar number voluntarily to the Company notified under first proviso to sub-section (1) of section 11A of the PML Act; or

      a. the proof of possession of Aadhaar number where offline verification can be carried out; or

      b. 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; or

      c. the KYC Identifier with an explicit consent to download records from CKYCR; and

b. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

c. 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 RE:

Provided that where the customer has submitted:

- proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.

- 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 as specified under Digital KYC Process.

- any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under Digital KYC Process

- KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR.

Provided that for a period not beyond such date as may be notified by the Government for a NBFC, instead of carrying out digital KYC, the Company 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.

In case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme, owing to injury, illness or infirmity on account of old age or otherwise and similar causes, the Company shall apart from obtaining the Aadhar 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.

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 subjected to periodic internal audit/inspection by the Company and shall be available for supervisory review.

Explanation 1: The Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per provision (i) above.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

KYC verification once done by one branch/office of the Company shall be valid for transfer of the account to any other branch/office, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

NOTE:

- PAN Card shall be verified electronically from NSDL so as to ascertain correctness of PAN Number and corresponding name appearing in Income Tax data base. The said verification may be carried out by the Company itself or through an independent Agency.
- Similarly, AADHAR, Driving License & Voters ID shall be verified through Independent Agency.
- Utility Bills and Passport will be used to verify address.
- Customer will electronically upload his selfie.
- Bank statement will be used to verify bank account number.

ANNEXURE 4

CUSTOMER IDENTIFICATION PROCEDURE

Certified documents or its equivalent e-documents that shall be obtained from the customers at the time of account opening are as below:

Customers	Documents
Individuals and Sole proprietors (Proof of identity and proof of residence)	One of the following certified physical documents or e-documents thereof viz., 1. Passport
	2. Aadhaar Card (mandatory for any subsidy benefit) or Proof of possession of Aadhaar issued by `UIDAI or E-Aadhaar.
	3. Voter's Identity Card issued by the Election Commission of India
	4. Driving License
	5. Job card issued by NREGA duly signed by an officer of the State Govt
	6. Letter issued by Registrar of National Population Register containing details of name and address. And Permanent Account Number (PAN) or Form No. 60 as per Income Tax Rules 1962 (Mandatory along with one of the OVDs) Provided that, 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. 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 Gazette notification or marriage certificate issued by the State Government, indicating such a change of name. In case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:

	(i) Utility bill (electricity, telephone, post-paid mobile phone, piped gas, water bill) not more than 2 months old (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; In case the OVD submitted 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 Provided further that the customer shall submit an updated OVD with the current address within a period of three months of submitting the above documents.
Sole Proprietorship Firm	Apart from Customer identification procedure as applicable to the proprietor any two of the following certified copy of documents or equivalent e-documents thereof in the name of the proprietary concern would suffice: (i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government. (ii) Certificate/ license issued by the municipal authorities under Shop and Establishment Act. (iii) Sales and income tax returns. (iv) CST/VAT/GST certificate (provisional/ final) (v) Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities.

	(vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax authorities. (viii) Utility bills such as electricity, water, and landline telephone bills In cases where the Company is satisfied that it is not possible to furnish two such documents, it would have the discretion to accept only one of those documents as activity proof. In such cases, the Company, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy that the business activity has been verified from the address of the proprietary concern.
Company	One certified copy of each of the following documents or the equivalent e-documents thereof: (i) Certificate of incorporation; (ii) Memorandum and Articles of Association; (iii) Permanent Account Number of the company; (iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; (v) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Number or Form 60 of the beneficial owners, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (vi) the names of the relevant persons holding senior management position; and

	(vii) the registered office and the principal place of its business, if it is different.
Partnership Firms	One certified copy of each of the following documents or the equivalent e-documents thereof: (i) Registration certificate; (ii) Partnership deed; (iii) Permanent Account Number of the partnership firm; (iv) One copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Number or Form 60 of the beneficial owners, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (v) the names of all the partners and (vi) address of the registered office, and the principal place of its business, if it is different.
Trusts & Foundations	One certified copy of each of the following documents or the equivalent e-documents thereof: i. Certificate of registration, if registered ii. Trust Deed iii. Permanent Account Number or Form No.60 of the trust iv. One copy of an OVD containing details of identify and address, one recent photograph and Permanent Account Number (PAN) or Form 60 of the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers/ directors Resolution of the managing body of the foundation/ association. v. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust vi. the address of the registered office of the trust; and vii. list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

	The Company shall ensure that trustees disclose their status at the time of commencement of an account-based relationship.
Unincorporated Association or Body of Individuals	One certified copy of each of the following documents or the equivalent e-documents thereof: i. Resolution of the managing body of such association or body of individuals ii. power of attorney granted to him to transact on its behalf iii. PAN or Form 60 of the unincorporated association or body of individuals iv. One copy of an OVD containing details of identify and address, one recent photograph and Permanent Account Number (PAN) or Form 60 of the person holding an attorney to transact on its behalf. Such other documents as may be required by Company to collectively establish the legal existence of such as association or body of individuals.

Direction for Selling Third party products:

If in the future, the Company acts as agent while selling third party products, it shall comply with the applicable laws/regulations, including system capabilities for capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers.

Video based Customer Identification Process (V-CIP)

BFIL may undertake live V-CIP to be carried out by its official for establishment of an account based relationship with a new individual customer, proprietor (in case of proprietorship firm), authorized signatories and Beneficial Owner (BO) (in case of Legal Entity (LE) customers), conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication and updation/ periodic updation of KYC for eligible customers, after obtaining his informed consent and shall adhere to the following stipulations:

A. V-CIP Infrastructure

1. BFIL shall comply with the RBI guidelines on minimum baseline cyber security and resilienceframework, as well as other general guidelines on IT risks.

2. BFIL shall have in-house infrastructure in its own premises and the V-CIP connection and interactionshall originate from its own secured network domain. BFIL shall also comply with the Outsourcing Guidelines issued by RBI for any technology related outsourcing activities.

3. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with BFIL only and all the data including video recording is transferred to BFIL's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of BFIL.

4. BFIL shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

5. The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

6. The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt

7. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with BFIL. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

8. BFIL shall regularly upgrade technology infrastructure including application software as well as workflows based on experience of detected / attempted / 'near-miss cases of forged identity. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

9. BFIL shall conduct necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities of V-CIP Infrastructure. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Any critical gap reported under this process shall be mitigated before rolling out its implementation. BFIL shall engage suitably accredited agencies as prescribed by RBI to conduct such tests periodically in conformance to internal / regulatory guidelines.

B. V-CIP Procedure

1. BFIL shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of BFIL specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

2. Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop / disconnection, fresh session shall be initiated.

3. The official of BFIL shall ensure that if there is a disruption in the V-CIP procedure, the same shall be aborted and a fresh session shall be initiated.

4. The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

5. Any prompting, observed at end of customer shall lead to rejection of the account opening process.

6. The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of workflow.

7. The authorised official of BFIL performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

    a. OTP based Aadhaar e-KYC authentication.

    b. Offline Verification of Aadhaar for identification

    c. KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer.

    d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi locker.

    BFIL shall ensure to redact or blackout the Aadhaar number.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, BFIL shall ensure that the XML file or QR code generation date is not older than 3 working days from the date of carrying out V-CIP.

Further, in line with the aforesaid prescribed period, BFIL shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, BFIL shall ensure that no incremental risk is added due to this.

8. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured. BFIL shall ensure that the economic and financial profile/information submitted by the customer is also confirmed from the customer while undertaking the V-CIP in a suitable manner.

9. BFIL shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi locker.

10. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

11. The authorised official of BFIL shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP, and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

12. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

13. BFIL shall comply with all such matters required under other statutes, such as the Information Technology (IT) Act.

C. V-CIP Records and Data Management

1. BFIL shall store the entire data and recordings in a system(s) located in India, in a safe and secured manner and shall bear time and date stamp for easy historical search.

2. BFIL shall follow the provisions of Record Management as contained in this Policy.

3. The activity log along with credential of the official performing V-CIP shall be preserved.

ANNEXURE 5

Risk Management

Risk Categorization: Indicative Guidelines

As per the KYC policy, for acceptance and identification, the Company's Customers would be categorized based on perceived risk, broadly into three categories – A, B & C. Category A would include High-Risk Customers, Category B would include Medium Risk Customers while Category C would include Low-Risk Customers.

None of the Customers will be exempted from the Company's KYC procedures, irrespective of the status and relationship with Company or its Promoters. The due diligence to be exercised would depend on the risk categorisation of the customers. Enhanced due diligence will be carried out in respect of customers falling in the medium and high-risk category.

The Company currently lends to salaried Indian resident. Board categorization is based on income, age profile, social loan quotient, credit bureau and other obligations of the customer. Individuals whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk by the Company. In such cases, the Policy may require that only the basic requirements of verifying the identity and location of the Customer are to be met. Customers that are likely to pose a higher-than-average risk to the Company will be categorized as medium or high risk depending on Customer's background, nature, location of activity, 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 Company may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

Customer risk category should include:

1. High risk customers typically include:
    a. Accounts opened in non-face to face mode until the identity of the customer is verified in face-to-face manner or through V-CIP.
    b. Non-resident customers
    c. High net worth individuals without an occupation track record of more than 3 years.
    d. Trust, charitable organizations, Non-Government Organization (NGO), organizations receiving donations.
    e. Companies having close family shareholding or beneficial ownership.
    f. Firms with sleeping partners.

g. Politically exposed persons (PEPs) of Indian/ foreign origin

h. Person with dubious reputation as per public information available.

i. Company name changed.

j. Irregular/Delay in compliance – GST, PF, etc

k. Any other risk perceived by Credit during assessment.

2. Medium Risk customer will include:

a. Salaried applicant with variable income/ unstructured income receiving Salary in cheque;

b. Self- employed professionals other than HNIs.

c. Self-employed customers with sound business and profitable track record for a reasonable period.

d. High Net worth individuals with occupation track record of more than 3 years.

e. Any other risk perceived by Credit during assessment.

3. Low Risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified, and all other person not covered under above two categories. Customer carrying low risk may include the following:

a. Salaried employees with well-defined salary structures.

b. People belonging to lower economic strata of the society whose accounts show small balances and low turnover.

c. People working with government owned companies, regulators and statutory bodies, MNC's, rated companies public sector units, public limited companies etc.

Important for Risk categorization:

- If the client falls under more than one Risk category, then higher Risk Category shall apply. E.g., If the client is in the Low-Risk category and also a PEP (i.e., High Risk category), then the Client would be considered in the High-Risk category.

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

ANNEXURE 6

Illustrative list of activities which would be construed as suspicious transactions.

- Activities not consistent with the customer's business, i.e., accounts with large volume of credits whereas the nature of business does not justify such credits.

- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
    - A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
    - Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
    - An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
- Certain Employees of the Company arousing suspicion:
    - An employee whose lavish lifestyle cannot be supported by his or her salary.
    - Negligence of employees/willful blindness is reported repeatedly.
- Some examples of suspicious activities/transactions to be monitored by the operating staff:
    - Multiple accounts under the same name
    - Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc.
    - There are reasonable doubts over the real beneficiary of the loan
    - Frequent requests for change of address

Version Control

Sr. No.	Version Control No.	Date created/ updated
1.	Version 1	21st April 2022
2.	Version 2	25th April 2024