ANTI MONEY LAUNDERING ("AML") / COMBATTING THE FINANCING OF TERRORISM ("CFT") KNOW YOUR CUSTOMER ("KYC") POLICY

PREAMBLE

The Reserve Bank of India ("**RBI**") vide its Master Direction dated February 25, 2016 bearing reference number RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 (as amended from time to time) ("**RBI Master Direction**") provides that all non-banking financial companies are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. All non-banking financial companies are mandated to take steps to implement the provisions of the Act and Rules, including operational instructions issued in pursuance of such amendments.

In compliance with RBI Master Directions, Progfin Private Limited (formerly known as Hytone Holdings Private Limited) (hereinafter referred to as the "**Company**") has adopted this AML / CFT / KYC policy at the meeting of the board of the Company broadly outlining the Company's approach to KYC, AML and CFT related matters ("**Policy**").

SCOPE AND APPLICABILITY

This Policy is applicable to all offices/ branches/ business outlets of the Company and covers all aspects of customer identification, customer acceptance, customer due diligence, risk profiling and on- boarding of customers of various categories within the regulatory framework, monitoring of transactions, organizational arrangements apart from maintenance of records, risk reviews and reporting obligations.

The operation of this Policy, unless specifically mandated by law or regulations, shall not result in the denial of financial facility/ service to members of the general public, especially those, who are financially or socially disadvantaged. No decision-making functions for determining compliance with KYC norms will be outsourced to a third party.

All principles of law as set out in RBI Master Direction are deemed to be incorporated by reference under this Policy. This Policy shall always be read in consonance with the requirements under RBI Master Direction and in the event of any conflict between the requirements under this Policy and the RBI Master Direction, Company shall ensure that it undertakes such action(s) as may be in furtherance of the RBI Master Direction.

ENFORCEMENT AUTHORITY

The effective implementation of the KYC Policy and all associated procedures rests with the Principal Officer of the Company.

PERIODIC REVIEW AND REPORTING

A periodic review of adherence to the KYC policy and regulations shall be carried out by the Board on a periodic basis.

COMPONENTS OF THE KYC POLICY:

The following are the key elements of the Company's KYC policy:

a) Customer Acceptance Policy;
b) Risk Management;
c) Customer Identification Procedures; and
d) Monitoring of Transactions

CUSTOMER ACCEPTANCE POLICY

The Company shall ensure that:

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

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

c) No transaction or account based relationship is undertaken without following the CDD procedure.

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

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

f) The Company shall apply the CDD procedure at the unique customer identification code ("**UCIC**") level. Thus, if an existing KYC compliant customer of a regulated entity ("**RE**") desires to open another account with the Company, there shall be no need for a fresh CDD exercise.

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

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

i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the United Nations Security Council ("**UNSC**") sanctions lists circulated by the RBI.

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

k) Where an equivalent e-document is obtained from the customer, the customer shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (as may be amended from time to time).

Company shall ensure that the requirements under this Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged. Customer Acceptance and on-boarding shall be based only on the customer's request.

RISK MANAGEMENT

The Company shall have a risk based approach for mitigation and management of the identified risk including controls and risks as detailed below in this Policy.

a) Customers shall be categorised as low, medium and high risk category based on the assessment and risk perception by the Company.

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

Collection of Information from different categories of customers as specified in this policy relating to the perceived risk shall be non-intrusive and respectful. The Company may use Financial Action Task Force ("**FATF**") Public Statement, the reports and guidance notes on KYC / AML issued by the Indian Banks Association ("**IBA**") and guidance note circulated to all cooperative banks by the RBI etc. in carrying out risk assessment.

The decision making functions of determining compliance with KYC norms, risk categorization and sign off on customer acceptance shall not be outsourced.

CUSTOMER IDENTIFICATION PROCEDURE ("CIP")

The Company shall undertake identification of customers in the following cases, in the context of its business model:

a) Commencement of an account-based relationship with the customer.

b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

c) Selling third party products as agents, payment of dues of credit cards / sale and reloading of prepaid/travel card, and any other product for more than Rs. 50,000/- (Rupees Fifty Thousand Only).

d) Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000/- (Rupees Fifty Thousand Only), whether conducted as a single transaction or several transactions that appear to be connected.

e) When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/- (Rupees Fifty Thousand Only).

f) Carrying out transactions including international remittance as may be applicable for a non- account-based customer, that is a walk-in customer

g) The Company shall ensure that introduction is not to be sought while opening accounts.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company, shall at its option, rely on customer due diligence done by a third party, subject to the following conditions:

a) Records or the information of the customer due diligence carried out by the third party is obtained within 2 (two) days from the third party or the unique number or code assigned to a customer is obtained from the Central KYC Records Registry ("**CKYCR**").

b) Adequate steps shall be taken by the Company to satisfy itself 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, 2002 ("**PML Act**").

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

e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

CUSTOMER DUE DILIGENCE ("CDD") PROCEDURE :

I. CDD Procedure in case of Individuals:

A. Procedure for obtaining Identification Information:

For undertaking CDD, the Company shall obtain the following information from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, 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 his / her Aadhaar number voluntarily to the Company; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any Officially Valid Document ("OVD") as detailed in Annex I or the equivalent e-document thereof containing the details of his identity and address; and

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

b) Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company:

Provided that where the customer has submitted,

i. Aadhaar number under clause (a) above to the Company, the Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility as and when that facility is provided by the Unique Identification Authority of India.

Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self- declaration to that effect to the Company.

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

iii. An equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (as may be amended from time to time) and any rules issues thereunder and take a live photo as specified under **Annex II**.

iv. 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 [1]digital KYC as specified under **Annex II**.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the Company may, if so covered by the notification, obtain a [2]certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. The CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the concurrent audit as mandated. 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.

The Company shall, where its customer submits a proof of possession of Aadhaar 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 proviso aforementioned. Further, 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.

B. Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the conditions as specified in the applicable RBI Master Direction on KYC & AML:

.

Video based Customer Identification Process (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorised 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. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP. The detailed process has been mentioned in **Annex III**.

1

C. Simplified procedure for opening accounts by the Company:

In case a person who desires to open an account is not able to produce documents, as specified above, the Company may at its discretion open accounts subject to the following conditions:

(a) The Company shall obtain a self-attested photograph from the customer.

(b) The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) The account shall remain operational initially for a period of twelve months, within which CDD as per the provisions of this Policy shall be carried out.

(d) Balances in all their accounts taken together shall not exceed Rs. 50,00,000/- (Rupees Fifty Lakhs Only) at any point of time.

(e) The total credit in all the accounts taken together shall not exceed Rs. 1,00,000/- (Rupees One Lakh Only) in a year. The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case directions (d) and (e) above are breached by him / her.

(f) The customer shall be notified when the balance reaches Rs. 40,00,000/- (Rupees Forty Lakhs Only) or the total credit in a year reaches Rs. 80,00,000/- (Rupees Eighty Lakhs Only) that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

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

I. CDD Measures for Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out in accordance with the procedures at Part I above.

In addition to the above, any two of the following documents or the equivalent e- documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

(a) Registration Certificate /licence issued by the municipal authorities under Shop and Establishment Act.

(b) Sales and income tax returns.

(c) (provisional/final) CST/VAT/ GST certificate

(d) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

(e) Importer Exporter Code ("**IEC**") issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

(f) 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.

(g) Utility bills such as electricity, water, landline telephone bills, etc.

In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/activity provided the Company undertakes contact point verification and collects such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

II. CDD Measures for Legal Entities

For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Certificate of incorporation
b) Memorandum and Articles of Association
c) Permanent Account Number of the company

d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
e) Documents, as specified hereinabove, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Registration certificate
b) Partnership deed
c) Permanent Account Number of the partnership firm
d) Documents, as specified hereinabove, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
e) .

For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Registration certificate
b) Trust deed
c) Permanent Account Number or Form No.60 (as defined in the Income Tax, 1961) of the trust
d) Documents, as specified hereinabove, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

For opening an account of an unincorporated association or a body of individuals which include unregistered trusts/ partnership firms/ societies, certified copies of each of the following documents or the equivalent e – documents thereof shall be obtained:

a) Resolution of the managing body of such association or body of individuals
b) Permanent Account Number or Form No. 60 (as defined in the Income Tax, 1961) of the unincorporated association or a body of individuals
c) Power of attorney granted to transact on its behalf
d) Documents, as specified hereinabove, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
e) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.

For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

a) Document showing name of the person authorised to act on behalf of the entity;
b) Documents, as specified in this Policy, of the person holding an attorney to transact on its behalf and
c) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

III. Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified in the following manner:

a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

c) Definition of beneficial owner has been provided in **Annex IV**.

ON-GOING DUE DILIGENCE

The Company 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; and the source of funds.
The extent of monitoring shall be aligned with the risk category of the customer:

a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in 6 (six) months, and the need for applying enhanced due diligence measures shall be put in place.

b) The transactions in accounts of marketing firms, especially accounts of multi-level marketing ("**MLM**") companies shall be closely monitored.

PERIODIC UPDATION OF KYC:

The Company will adopt a risk-based approach to periodically update the KYC of its customers. Periodic updation shall be carried out at least once in every 2 (two) years for high risk customers, once in every 8 (eight) years for medium risk customers and once in every 10 (ten) years for low risk customers from the date of opening of the account/ last KYC updation. The details of periodic updation for individual customers and non-individual customers are given in **Annex V**.

In case of existing customers, the Company shall obtain the Permanent Account Number or equivalent e- document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which the Company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, the Company 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 the Company gives in writing to the Company that he does not want to submit his Permanent Account Number or equivalent e- document thereof or Form No. 60 (as defined in the Income Tax, 1961), the Company 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.

For the purpose of this Clause, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the provisions of this Clause. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

ENHANCED AND SIMPLIFIED DUE DILIGENCE PROCEDURE

I. Enhanced Due Diligence:

a) Accounts of Politically Exposed Persons ("**PEP(s)**"):

The Company shall establish a relationship with [3]PEPs provided that:

i. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

ii. the identity of the person shall have been verified before accepting the PEP as a customer;

iii. the decision to open an account for a PEP is taken at a senior level in accordance with the Company's Customer Acceptance Policy;

iv. all such accounts are subjected to enhanced monitoring on an on-going basis;

v. 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;

vi. the CDD measures as applicable to PEPs including enhanced monitoring on an on- going basis are applicable.

The above due diligence measures shall be applicable to accounts where a PEP is the beneficial owner.

RECORD MANAGEMENT

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of the PML Act and its Rules. The Company shall:

a) maintain all necessary records of transactions between the Company and the customer for at least 5 (five) years from the date of transaction;

b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least 5 (five) years after the business relationship is ended;

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

d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("**PML Rules**"); 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.

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

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it was denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction.

f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 of PML Rules in hard or soft format.

REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA ("FIU-IND")

(a) The Company shall furnish to the Director, Financial Intelligence Unit-India, information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. The Director, FIU-IND, shall have powers to issue guidelines to the Company for detecting transactions under the applicable rules and also directions about the form of furnishing information and to specify the procedure and the manner of furnishing information.

(b) The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic cash transaction reports ("**CTR**") / Suspicious transaction reports ("**STR**") which FIU-IND has placed on its website shall be made use of by the Company till it installs/adopts suitable technological tools for extracting CTR/STR from live transaction data. To the extent any of the branches of the Company may not be fully computerised, suitable arrangement shall be put in place to cull out the transaction details from such branches feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website: http://fiuindia.gov.in.

(c) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

(d) 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.

REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS- COMMUNICATIONS FROM INTERNATIONAL AGENCIES

I. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

(a) The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 ("**UAPA**") 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. The details of the two lists are as under:

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

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

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

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

(b) 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 2, 2021.

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

(c) Freezing of Assets under Section 51A of UAPA, 1967

The procedure laid down in the UAPA Order dated February 2, 2021, shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

IV. Jurisdictions that do not or insufficiently apply the FATF Recommendations

i. FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

ii. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements. The process referred to in Secrecy Obligations and Sharing of Information *(as describedhereinbelow)* do not preclude the Company from having legitimate business transactions with the countries and jurisdictions mentioned in the FATF statement.

iii. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to the RBI / other relevant authorities, on request.

Secrecy Obligations and Sharing of Information:

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

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

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

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. Interest of company requires disclosure, and
iv. Where the disclosure is made with the express or implied consent of the customer.

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

(e) 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.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

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

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. While preparing the internal risk assessment, the company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.

(b) The risk assessment by the company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

The company shall apply a Risk Based Approach ("**RBA**") for mitigation and management of the identified risk. Further, the company shall monitor the implementation of the controls and enhance them if necessary.

MISCELLANEOUS POINTS

I. CDD Procedure and sharing KYC information with Central KYC Records Registry

(a) The Company shall capture the KYC information for sharing with the Central KYC Records Registry 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.

(b) The Company shall capture the KYC information for sharing with the Central KYC Records Registry in the manner mentioned in the Rules, as required by the revised KYC templates prepared for individuals and Legal Entities ("**LE/s**") as the case may be.

(c) The Company shall upload KYC records pertaining to accounts of LEs opened on or after April 01, 2021 with CKYCR.

(d) The Company shall capture customer's KYC records and upload onto Central KYC Records Registry within 10 (ten) days of commencement of an account-based relationship with the customer.

(e) Once [4]KYC Identifier is generated by CKYCR, the same will be communicated to the customer.

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

i. there is a change in the information of the customer as existing in the records of CKYCR or;

ii. the current address of the customer is required to be verified or;

iii. it is considered as necessary by the Company 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.

(g) The Company shall upload/ update the KYC data pertaining to accounts opened prior to CKYC implementation dates at the time of periodic updation or earlier when the updated KYC is obtained from the customer.

II. Compliance with reporting requirement under Foreign Account Tax Compliance Act ("**FATCA**") and Common Reporting Standards ("**CRS**") as applicable to the Company. The Company will ensure strict adherence to the reporting requirements under FATCA and CRS. Towards this end, it will constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

III. Allotment of Unique Customer Identification Code (UCIC) to customers.

A Unique Customer Identification Code ("**UCIC**") shall be allotted while entering into new relationships with individual customers as also the existing customers by the Company. The Company shall, at their option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third-party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

IV. Permanent account number ("**PAN**") or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B as applicable and as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

V. Hiring of employees and employee training:

Adequate screening mechanism, , as an integral part of their personnel recruitment / hiring process shall be put in place.

.On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML / CFT policy. The focus of the training shall be different for 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 persons adequately trained and well-versed in AML / CFT policies of the Company, regulation and related issues shall be ensured.

VI. Appointment of Principal Officer:

The Company shall appoint a Principal Officer, who will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

VII. Appointment of Designated Director:

The Company shall appoint a Designated Director in terms of the obligations under the Prevention of Money Laundering (Amendment) Act, 2012 and clarification issued vide RBI Circular DNBR.PD.CC.No.022/03.10.042/2014-15 dated March 16, 2015 and subsequent modification thereof.

VIII. Collection of Account Payee Cheques and cash deposits
Account payee cheques for any person other than the payee constituent of the Company shall not be collected. Ordinarily, the Company will not entertain cash transactions by its customers. In exceptional cases where cash transactions are allowed, the Company will maintain proper records of the same and capture data for the CTR report as may be applicable.

OUTSOURCING OF ACTIVITIES FOR DETERMINING COMPLIANCE WITH KYC NORMS

The Company, as a policy will not outsource the compliance functions and decision-making functions such as determining compliance with KYC norms to a third party. However, in line with the Company's outsourcing policy and to the extent permitted in terms of paragraph 2 of **Annexure XXV** of the RBI Master Directions for NBFC-ND-SI, the Company may outsource all or any of the decision-making functions relating to determining of compliance with KYC norms to entities

within its promoter [5]group. However, in doing so, the Company acknowledges that that outsourcing of any activity by the Company does not diminish its obligations, as the onus of compliance with regulatory instructions rests solely with it.

POLICY VALIDITY AND REVIEW

This policy would be reviewed and updated at annual interval or earlier as considered necessary. Further, as and when RBI modifies Master Direction for KYC, the same will be incorporated in the Company's KYC policy and implemented from effective date of such directions. The Board will be intimated about such modification in the subsequent board meeting.

IMPLEMENTATION

This Policy shall be effective from the date of adoption by the Board.

AMENDMENT

This Policy shall be amended and/or restated and updated from time to time and such amendments and/or restatements and updation shall be effective from the date of adoption by the Board.

Annex I - OVD

"Officially Valid Document" ("**OVD**") means the passport, the driving licence, 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 NationalPopulation 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 maysubmit 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 followingdocuments 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

ii.

iii. of any service provider (electricity,telephone, post-paid mobile phone, piped gas, water bill);

iv. property or Municipal tax receipt;

v. pension or family pension payment orders ("**PPO(s)**") issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

vi. letter of allotment of accommodation from employer issued by State Government or CentralGovernment Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements withsuch employers allotting official accommodation;

(c) The customer shall submit OVD with current address within a period of three months ofsubmitting 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 letterissued 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 thereis a change in the name subsequent to its issuance provided it is supported by a marriage certificateissued by the State Government or Gazette notification, indicating such a change of name.

Annex II - Digital KYC Process

(a) The Company may develop an application for digital KYC process which shall be made available atcustomer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application.

(b) The access of the application shall be controlled by the Company and it shall be ensured that the same is not used by unauthorized persons. The application shall be accessed only through login-idand password or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

(c) The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company orvice-versa. The original OVD shall be in possession of the customer.

(d) The Company must ensure that the live photograph of the customer is taken by the authorized officerand the same photograph is embedded in the Customer Application Form ("**CAF**"). Further, the system application of the Company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee code (assigned by the Company) and date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

(e) The application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The backgroundbehind the customer while capturing live photograph should be of white colour and no other personshall come into the frame while capturing the live photograph of the customer.

(f) Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where [6]offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in themobile device shall be there while capturing the live photograph of the original documents.

(g) The live photograph of the customer and his original documents shall be captured in properlight so that they are clearly readable and identifiable.

(h) Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response ("**QR**") code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar / e- Aadhaar.

(i) Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company- shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

(j) Subsequent to all these activities, the application shall give information about the completion of the process and submission of activation request to activation officer of Company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

(k) The authorized officer of the Company shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) livephotograph of the customer matches with the photo available in the document.; and (iii) all of thenecessary details in CAF including mandatory field are filled properly.

(l) On successful verification, the CAF shall be digitally signed by authorized officer of the Company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Annex III: V - CIP Process

The Company may undertake [7]V-CIP to carry out:

i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners ("**BO/s**") in case of Legal Entity customers. Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in the Policy, apart from undertaking CDD of the proprietor.

ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per the Policy.

iii. Updation / Periodic updation of KYC for eligible customers.

The Company shall adhere to the following minimum standards for undertaking V-CIP:

I. V-CIP Infrastructure

i. The Company shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks.The technology infrastructure shall be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines.

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

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

iv. The video recordings shall 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.

v. 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 the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

vii. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests shall also be carried out periodically in conformance to internal / regulatory guidelines.

viii. The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application shall be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

II. V-CIP Procedure

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

ii. If there is a disruption in the V-CIP procedure, the same shall be aborted and a fresh session initiated.

iii. 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.

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

v. 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 shall be factored in at appropriate stage of work flow.

vi. The authorised official of the Company 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 14.1, using the KYC identifier provided by the customer;
d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker;

The Company shall ensure to redact or blackout the Aadhaar number.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 (three) days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that the video process of the V-CIP is undertaken within three 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, the Company shall ensure that no incremental risk is added due to this.

viii. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

ix. The Company 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 Digilocker.

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

xi. The authorised official of the Company 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.

xii. The ultimate responsibility for customer due diligence shall be with the Company.

xiii. 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.

xiv. All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

III. V-CIP records and data management:

i. The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management shall also be applicable for V-CIP.

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

Annex IV - Beneficial Owner

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

For the purpose of this sub-clause-

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

ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

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

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

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

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

Annexure V - Periodic Updation

(a) Individual Customers:

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 Company, 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 Company, 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 or the equivalent e-documents thereof, as defined in Annexure II, for the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, can be applied post approval from the Board.

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.

(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 it 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 the Company. 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.

v. The Company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, 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., can be applied only post approval from the Board.

vi. The Company shall ensure that its KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers shall be avoided, unless warranted by specific regulatory requirements.