SUB AUA SERVICES ENGAGEMENT AGREEMENT - Version 1.5

This Sub AUA Services Engagement Agreement is made at Bangalore on this 28 day of December, 2016 (**"Agreement"**) between:

Khosla Labs Private Limited, a company incorporated under the Companies Act, 1956 and having its registered office at #18/2A,GRS Towers, Second Floor, Above Spencer's Hypermarket, Sarjapur Road, Bangalore - 560102, Karnataka (hereinafter referred to as **"KLPL"**, which expression, unless repugnant to the context or meaning thereof, shall mean and include its successors and assigns) of **One Part**;

AND

Tamilraja, an individual/proprietor/sole-owner having his/her permanent address at chennai aadhambakkam tamilnadu -600088 (hereinafter referred to as **"Sub-AUA"**, which expression, unless repugnant to the context or meaning thereof, shall mean and include his/her successors and assigns) of **Other Part**;

KLPL and Sub-AUA are hereinafter individually referred to as 'Party' and collectively as 'Parties'.

WHEREAS:

(A) KLPL has been authorized to act as an Aadhaar Authentication Agency (" **AUA** ") by the UIDAI. KLPL further engages with its partner ASAs for the provision of secured network connectivity between the CIDR and the AUA for enabling Aadhaar Authentication Services.

(B) The Sub-AUA is desirous of using the Aadhaar Services provided by UIDAI, as facilitated by KLPL so as to provide Aadhaar Enabled Services to its beneficiaries, clients and customers and is entering into this arrangement with KLPL to engage as a Sub-AUA.

(C) The Sub-AUA is aware of, and agrees that:

   a. the Aadhaar Services are subject to limitations, including as posed by technology, and KLPL does not represent and warrant the same to be defect free; and

   b. the Aadhaar Services are provided on an 'as is' basis, without any express or implied warranties in respect thereof, and KLPL does not assume any responsibility or liability for any damage, whether direct, indirect, incidental or consequential, arising as a result of the use of the Aadhaar Services.

NOW THEREFORE, IN CONSIDERATION OF THE MUTUAL COVENANTS AND PROMISES SET FORTH HEREIN, THE RECEIPT AND SUFFICIENCY OF WHICH IS HEREBY ACKNOWLEDGED, THE PARTIES HEREBY COVENANT AND AGREE AND THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. DEFINITIONS

1.1. **Aadhaar** means the 12 digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India.

1.2. **Aadhaar Authentication Services** shall mean the authentication services provided by UIDAI where the personal identity information of / data of an Aadhaar Holder (who is a beneficiary, customer, employee or associate of the Sub-AUA is matched with their personal identity information / data that is stored in the CIDR in order to provide Aadhaar Enabled Services to such Aadhaar Holder.

1.3. **Aadhaar Enabled Services** shall mean services provided by the Sub-AUA to Aadhaar Holder, using the Aadhaar Authentication Services of UIDAI.

1.4. **Aadhaar Holder** shall mean an individual who holds an Aadhaar Number.

1.5. **Aadhaar Number** shall mean the unique identification number issued to resident of India by UIDAI.

1.6. **Aadhaar Services** shall mean the Aadhaar Authentication Services.

1.7. **ASA** shall mean the Authentication Service Agency.

1.8. **Authentication Device(s)** shall mean a terminal or device from where the SubAUA carries out its service/business functions and interacts with Aadhaar Holders, by seeking authentication of Aadhaar Holders identity to enable the SubAUA's business function.

1.9. **Biometric Information** shall mean ten finger prints and iris image, captured by UIDAI, as a part of the enrolment process for issuance of Aadhaar Number.

1.10.**Central Identity Data Repository** or **CIDR** shall mean a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto.

1.11.**Confidential Information** shall mean any information which is considered confidential in terms of Clause 9 of this Agreement and shall include, but not limited to, information such as Aadhaar Number, name, address, age, date of birth, relationships and other demographic information, as also, biometric information such as finger print and iris scan of a resident of India.

1.12.**Law(s)** shall mean all applicable laws, by-laws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any governmental authority or person acting under the authority of any governmental authority, whether in effect or which may come into effect in the future.

1.13.**Personal Identity Data or PID** refers to Aadhaar-based personal identity data / information including Biometric Information and demographic information as well as OTP used for authentication.

1.14.**UIDAI** shall mean the Unique Identification Authority of India, an authority set up by the Planning Commission, Government of India, vide Notification dated

28 January, 2009, and as at the Effective Date, having its address at 3rd Floor, Tower II, Jeevan Bharati Building, Connaught Circus, New Delhi-110001

2. **SCOPE**

2.1. Annexure A shall capture details of the services to be availed of and the purposes for which such services will be used.

2.2. It is clarified that the Sub-AUA will not be permitted to engage in transactions other than as set out in Annexure A.

2.3. The scope set out in Annexure A may be amended subject to mutual agreement between the parties.

3. **TERMS AND CONDITIONS OF APPOINTMENT AS SUB-AUA**

3.1. It is hereby mutually agreed between the Parties that the rights and obligations of the Sub-AUA under this Agreement, are non-transferable and non-assignable whether by sale, merger, or by operation of Law, except with the express written consent of KLPL

3.2. The Sub-AUA confirms and represents that it shall be responsible to UIDAI for all the Aadhaar authentication related aspects for all authentication requests which it transmits to the CIDR.

3.3. The Sub-AUA understands and agrees that the Aadhaar Services shall be provided at the sole discretion of UIDAI, which reserves the right to add, revise, suspend in whole, or in part any of the Aadhaar Authentication Services, at any time, in its sole discretion for any reason whatsoever.

3.4. The SubAUA hereby unequivocally agrees that all infrastructure, including backend infrastructure, such as hardware, equipment servers, databases etc. required for the purpose of Aadhaar authentication shall be based in the territory of India.

3.5. The SubAUA shall access data of an Aadhaar Holder solely in accordance with the policy of the UIDAI.

3.6. The SubAUA undertakes that the preproduction environment is used only for demonstration or testing purpose and shall not be used for commercial purposes at any time.

4. **RESPONSIBILITIES AND OBLIGATIONS**

4.1. **KLPL's Responsibilities and Obligations**

4.1.1. KLPL is authorized by UIDAI to act as an Authentication User Agency and in such capacity to avail of Aadhaar Services and to provide UIDAI-compliant network connectivity as a service to sub-authentication user agencies and transmit authentication requests to an ASA and CIDR.

4.1.2. In cases where the authentication devices are operated by AUA's personnel (or personnel of their agents), the AUA is responsible for ensuring that the operating personnel who are adequately trained to conduct Aadhaar-based authentication in compliance with UIDAI's requirements.

4.1.3. When KLPL engages with the Sub AUA, it shall generate a Sub AUA Code to identify the specific Sub AUA. When transmitting authentication requests from the Sub AUA, KLPL will always include the Sub AUA Code so that Aadhaar transaction logs can track the origin of all authentication.

4.1.4. KLPL shall take responsibility on behalf of the Sub AUA for the standards to be maintained regarding security, infrastructure, processes, devices and other aspects as specified by UIDAI. The AUAs shall take responsibility on behalf of their Sub AUAs for completeness of the authentication.

4.1.5. KLPL shall not be responsible to the Sub AUA for any faulty/false/ incorrect transactions or any incorrect responses received from the UIDAI.

4.1.6. KLPL shall inform ASAs of any termination of contracts with Sub AUAs.

4.2. **Sub-AUA's responsibilities and obligations**

4.2.1. The Sub AUA who is seeking to use Aadhaar Services to enable a specific service/business function is solely responsible for the choice of authentication type(s). The choice of the Authentication type shall be the sole decision of the Sub AUA, and no other entity, including UIDAI, Authentication Service Agency and Aadhaar Holder shall have any role in this decision of Sub AUA.

4.2.2. The Sub AUA should obtain consent from the individual before collecting his identity information for the purposes of authentication. The sample format is as set out in Annexure C.

4.2.3. The Sub AUA should ensure that the identity information of an individual is only used for submission to the CIDR for authentication.

4.2.4. The Sub AUA should inform the individual of the following with respect to his identity information for authentication:

4.2.4.1 The nature of information that may be shared upon authentication

4.2.4.2 The uses to which the information received during authentication may be put by the requesting entity.

4.2.4.3 Alternatives to submission of identity information to the requesting entity.

4.2.5. The consent of the individual may be obtained by the requesting entity in physical or electronic form.

4.2.6. The requesting entity must ensure that the consent form is made available to the Aadhaar holder in local language as well.

4.2.7. The SubAUA is requested to make necessary changes in their front end applications for obtaining the consent. Till the time the required changes are not implemented in the front end client application, the process of obtaining consent and informing the purpose of collecting biometric and identity information may be completed through physical forms.

4.2.8. It is hereby clearly understood by the SubAUA that KLPL shall have no responsibility or liability in relation to failures that may take place during the Aadhaar Authentication.

4.2.9. The SubAUA understands that the data will be provided in a manner conformant to the standards and processes described in the Demographic Data Standards and Verification Procedure (DDSVP) Committee Report;

4.2.10. The SubAUA understands that the data provided shall conform to Section 3 (Authentication of electronic Records), Section 4 (Legal recognition of electronic records), Section 5 (Legal recognition of digital signatures) and Section 6 (Use of electronic records and digital signatures in Government and its agencies) of the Information Technology Act, 2000;

4.2.11. The SubAUA shall maintain logs/records of obtaining the consent of the resident obtained in Section 8(2)(b) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,2016 for a time period specified by UIDAI and allow access to UIDAI or any entity authorized by it to the related records. The Sub AUA shall maintain the logs/records of the consent

4.2.12. The Sub AUA assumes complete responsibility with regard to its network connectivity with KLPL and UIDAI shall have no responsibility in this regard.

4.2.13. The Sub AUA assumes complete responsibility for all transactions and also undertakes to ensure that all the transactions will be used for carrying out activities that are compliant with all applicable laws, regulations, rules, guidelines etc.

4.2.14. The Sub AUA shall establish and maintain necessary authentication related operations, including systems, processes, infrastructure, technology, security, etc., which may be necessary for using Aadhaar Authentication Service, in compliance with standards and specifications, issued by UIDAI from time to time.

4.2.15. KLPL and the Sub AUA shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners)which are duly registered with/approved/ certified by UIDAI or an agency appointed by UIDAI for this purpose.

4.2.16. Both Parties understand the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which conform to the authentication type adopted by the Sub AUA, and UIDAI shall have no role to play in this regard, and shall have no liability or responsibility in this respect.

4.2.17. The Sub AUA shall ensure that the persons employed by it for providing Aadhaar Enabled Services and for maintaining necessary systems, infrastructure, processes, etc. in this regard, possess requisite qualifications for undertaking such works. The Sub AUA shall be responsible for ensuring that such personnel are suitably and adequately trained to conduct Aadhaar Enabled Services, in compliance with specifications and standards prescribed by UIDAI from time to time.

4.2.18. The Sub AUA shall, at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed

there under, from time to time, in so far as the same has application to its operations in accordance with this Agreement, and also with all other Laws, rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security and management, data storage, sharing and data protection, as also with the National Identification Authority of India Bill, as and when the same in enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device.

4.2.19. The Sub AUA shall, at all times, comply with the provisions of all applicable laws, regulations, rules, guidelines etc.

4.2.20. The Sub AUA shall comply with all applicable antibribery and corruption laws. The SubAUA understands that violation of this clause will constitute a material breach of this agreement.

4.2.21. The Sub AUA hereby unequivocally agrees that the use of the Aadhaar Enabled Services shall not, in any manner, whether direct or indirect, be used for purposes that are antigovernment or antiState or discriminatory or related to money laundering or in contravention of any Laws.

4.2.22. The Sub AUAs shall maintain logs of all authentication a transactions processed by it, capturing the complete details of the authentication transaction such as the Aadhaar number, transaction code, authentication type, requesting AUA, requesting authentication device, date and timestamp, etc. ,as prescribed by UIDAI from time to time, and shall retain the same for a duration as prescribed by UIDAI from time to time but shall not, store the Aadhaar Personal Identity Data of the Aadhaar Holder (PID) except in accordance with applicable policies of the UIDAI and/or the Government of India. The Sub AUA understands and agrees that the logs maintained by it shall not be shared with any individual or entity, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

4.2.23. The storage of data shall comply at all times with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

4.2.24. In case of any investigations around authentication related fraud(s) or dispute (s), the Sub AUA shall extend full cooperation to UIDAI, and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource / information, etc. of or pertaining to its Authentication Device.

4.2.25. The Sub AUA unequivocally agrees that all applications used by it in running its Aadhaar authentication operations shall be duly certified/ approved by UIDAI or an agency appointed/ approved by UIDAI (as and when UIDAI creates a certification mechanism for certifying Aadhaar enabled applications),. In the event the already certified/ approved applications employed by the Sub AUA undergo modifications, the

Sub AUA shall deploy the modified applications only after renewed certification/ approval from UIDAI.

4.2.26. The SubAUA shall obtain consent from the Aadhaar Holder, for using the Aadhaar number and Biometric information for providing the Aadhaar Enabled Services.

4.2.27. The SubAUA hereby unequivocally agrees that it shall, establish network connectivity, through KLPL, to the CIDR in compliance with all the specifications and Standards prescribed by UIDAI, from time to time. The Sub AUA assumes complete responsibility with regard to its network connectivity to KLPL.

4.2.28. The SubAUA shall establish and maintain necessary authentication related operations, including their own systems, process, infrastructure, technology, security, etc., which may be necessary for providing Aadhaar Enabled Services, in compliance with standards and specifications, issued by UIDAI from time to time.

4.2.29. The SubAUA shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners) which are duly registered with, approved/ and certified by UIDAI or an agency appointed by UIDAI for this purpose. The SubAUA understands the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which confirm to the authentication type adopted by the SubAUA, and KLPL shall have no role to play in this regard, and shall have no liability or responsibility in this respect.

4.2.30. The SubAUA shall maintain logs of all authentication transactions processed by it, capturing the complete details of the authentication, such as the Aadhaar number against which authentication is sought authentication package, date and timestamp, etc. as prescribed by UIDAI from time to time but shall not, in any event, capture the PID information and shall retain the same for a duration, specified by UIDAI from time to time. As set out above, the SubAUA understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need basis, and that the storage of the logs maintained by it shall comply with all the relevant Laws, rules and regulations, including, but not limited to, the Information Technology Act 2000 and the Evidence Act 1872.

4.2.31. The SubAUA shall not allow for any other organization/individual to use the services as provided by KLPL. The SubAUA understands that the services provided are specific to the SubAUA and cannot be transferred/ subleased or availed of by /for the benefit of/for the use of any other entity.

5. **REPRESENTATION, COVENANTS AND WARRANTIES OF KLPL AND the Sub-AUA:**

KLPL and the Sub-AUA hereby represent and warrant that:

5.1. They have all requisite powers and authority and have taken all actions necessary to execute, deliver, and perform its obligations under this Agreement.

5.2. This Agreement has been validly executed by the Parties and constitutes a valid agreement binding both the Parties and enforceable in accordance with the Laws of India.

5.3. All information communicated by both the Parties to each other for the purpose of this Agreement is true, correct and complete and is not misleading in letter or in spirit whether by reason of omission to state a material fact or otherwise.

5.4. Neither the making or performance of this Agreement nor compliance with its terms will be in violation of any law or conflict with or result in the breach of or constitute a default or require any consent under any decree, order, judgment, execution, claim, settlement or any other instrument to which either Party is a party or by which either Party is bound and no such decree, order, judgment, execution, claim, settlement or other instrument exists against KLPL or the Sub-AUA.

5.5. Both Parties shall at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed there under, from time to time, in so far the same has application to its operations in accordance with this Agreement, and also with all other Laws rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security and management, data storage, sharing and data protection, and also with the National Identification Authority of India Bill, as and when the same is enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device and in all its operations including but not limited to the operations involving the collection, storage and use of all biometric information and Personal Identity Data.

6. **PAYMENT & SETTLEMENT TERMS:**

6.1. KLPL shall charge the fees per transaction in the manner as set out in Annexure B.

6.2. KLPL may change the applicable fees at any time it so deems fit. The Sub AUA will be notified upon such change of applicable fees.

7. **PRIVACY POLICY**

KLPL has in place a Privacy Policy that sets out the treatment of the information collected in the provision of the Aadhaar Authentication Services. An extract of the Privacy Policy has been reproduced below. For the most recent version of the Privacy Policy, please visit the Aadhaar Bridge/Aadhaar Connect webpage.

7.1. **Information Collected**

7.1.1. In the provision of access to the Aadhaar Authentication Services, KLPL may collect a host of information including cookies, IP addresses, geolocations, browser information etc.

7.1.2. The information so collected may pertain to a natural person or a corporation/entity availing of the Aadhaar Authentication Services

7.1.3. KLPL is committed to protecting the personal information of customers and strives to maintain the privacy of all personal information that KLPL will have access to.

Personal information refers to any information from which your identity is apparent or can be reasonably ascertained. For the purpose of this policy, sensitive personal data or information has been considered as a part of Personal Information.

Together all such information being collected shall be referred to as the Information.

7.2. **Utilisation of the Information**

The Information collected will be used for the following purposes:

- Verify the identity of the customer (in line with the standards as expected by the UIDAI)

- Complete the on boarding procedure for a customer of Aadhaar Bridge

- Complete transactions effectively and bill for Aadhaar Bridge Services

- Respond to requests for service or assistance

- Perform market analysis, market research, business and operational analysis.

- Internal assessments, operations and related activities

- Ensure adherence to legal and regulatory requirements for prevention and detection of frauds and crimes

- Information collected from cookies and other technologies, like pixel tags, to improve customer experience.

7.3. **Disclosure of Information**

7.3.1. Internal Use: KLPL and its employees may utilise the Information for the purposes as set out in the 'Utilisation of the Information' section.

7.3.2. Authorised Third Parties: KLPL may at its discretion employ, contract or include Third Parties external to itself for strategic, tactical and operational purposes. Such sharing of Information is governed by contractual agreements that are in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. The agreements ensure that the Information can be utilised by the Third Party only in a manner and for purposes that are specifically contemplated by us in the governing agreement.

7.3.3. Government agencies: Khosla Labs Private Limited may share any and all parts of the Information with Government agencies, administrative bodies, authorised law enforcement agencies, court, regulatory/governmental authority or any other organisation, individual or entity for the following reasons:

- Verification of identity

- Prevention, detection, investigation including but not limited to cyber incidents, prosecution and punishment of offences

- To comply with any applicable law, order, regulation, or government request

- To enforce applicable Terms of Service, including investigation of potential violation

- To detect, prevent, or otherwise address fraud, security or technical issues

- For any other purpose as required by law, judicial or administrative order or regulation.

8. **INDEMNITY AND LIMITATION OF LIABILITY**

   8.1. KLPL shall not be liable for any errors, misrepresentations or false entries with respect to the requests made by the Sub AUA.

   8.2. The Sub AUA will be held responsible for all requests made and also will be liable for the consequences of such errors in the requests.

   8.3. It is hereby mutually agreed between the Parties that KLPL and its affiliates shall not be liable for any unauthorized transactions occurring through the use of Aadhaar Authentication Services by the Sub AUA. The Sub AUA hereby fully indemnifies and holds harmless KLPL and its affiliates against any Losses incurred by KLPL and/ or its affiliates as result thereof.

   8.4. In the event of a Third Party (including the UIDAI) bringing a Claim against KLPL and its affiliates in relation to, or as a consequence of, the use of Aadhaar Authentication Services by the Sub-AUA, the Sub-AUA shall:

       8.4.1 defend and / or assist KLPL and its affiliates in defending, at its own costs, such Claim, either in a legal proceeding or otherwise;

       8.4.2 fully indemnify and hold harmless KLPL and its affiliates at all times, against all Losses arising out of or incurred by reason of any breach by the other Party Entities of the terms and conditions or its appointment or its obligations under this Agreement; and

       8.4.3 fully indemnify and hold harmless the Party at all times, against all Losses arising out of or incurred by reason of any infringement of intellectual property rights of any Third Party in connection with the use of the Aadhaar Authentication Services, irrespective of whether or not the Party incurs any liability in this regard by virtue of any judgment of a court of competent jurisdiction.

9. **CONFIDENTIALITY:**

   9.1. Except as specifically set out in this Agreement, no communication concerning the terms of this Agreement shall be made or caused to be made before or after the execution of this Agreement, by both Parties without mutual consent.

   9.2. Both Parties have agreed that, save and except with the prior written consent of the other Party:

       9.2.1. On and from the date of this Agreement, the contents of this Agreement and all information, which a Party may obtain from the other Party pursuant to this Agreement (hereinafter referred to as "Confidential Information") shall be kept confidential and shall not be disclosed by either Party to any third party.

       9.2.2. Upon the expiry of the term of this Agreement or the termination of this Agreement, neither Party shall issue any adverse official written

communication relating to such termination or the factum of this Agreement.

9.2.3. However, the Parties may under certain circumstances and if it is essential for the assessment of the Transaction to disclose Confidential Information, may disclose such Confidential Information to its employees, and advisors (including without limitation, attorneys, accountants, consultants, bankers, financial advisors, or their representatives) whose knowledge of the Confidential Information is essential. In such event, the Parties shall disclose the confidential nature of such information and require all such employees/advisors/other persons to maintain confidentiality, either by virtue of their terms of employment/engagement with, or the internal company policy of the Parties.

9.3. Upon the expiration, cancellation or termination of this Agreement, either Party shall forthwith stop using and, return or destroy all Confidential Information, documents, manuals and other materials (including copies thereof) provided by the other Party. Upon request, the receiving Party shall send disclosing Party a certificate specifying that all the Confidential Information, documents, manuals and other materials have either been destroyed or returned.

9.4. The above clause shall survive for the period of three years after the termination of the Agreement.

10. **TERM**

10.1. This Agreement shall commence from the date of entering into this Agreement (" **Effective Date**") and shall remain continuously in force for a period of three (3) years thereafter (" **Term** "), until and unless otherwise terminated by either Party in terms of Clause 13 herein below, any time after six (6) months from the Effective Date (" **Lock-in Period** "), or renewed by the Parties in terms hereof.

10.2. The engagement shall be deemed automatically renewed upon availing of the services.

10.3. The renewal shall be for incremental one year periods.

11. **TERMINATION:**

11.1. Subject to the Lock-in Period, either Party shall have the option to terminate this Agreement at any time by giving thirty (30) days advance notice in writing to that effect to the other Party.

11.2. The Parties have right to terminate this Agreement forthwith by a notice in writing to the other Party, if other Party in any of the following conditions:

11.2.1 fails to comply with the Standards or the decision and directions issued by UIDAI, from time to time, with regard to the interpretation and enforcement of the Standards;

11.2.2 is in breach of its obligations under this Agreement;

11.2.3 uses the Aadhaar Authentication Services for any other purpose other than those as communicated to Khosla Labs Private Limited;or

11.2.4 has violated any law under which its right to business may cease and has failed to remedy the breach within seven (7) days of notice.

11.3. Each Party shall have the option to terminate this Agreement, by giving notice in writing, in the event that any other Party becomes insolvent, goes into liquidation or a liquidator is appointed to wind up the Company.

11.4. This Agreement shall stand terminated automatically if the business of either Party becomes illegal/unlawful/banned by the law of the land or if either Party indulges in any illegal act or practice that makes its business illegal/ unlawful/banned or if any transaction has taken place for which either Party was responsible which results directly or indirectly in Money Laundering activities or financing of terrorists activities. Neither Party shall be liable for such activities/ transactions nor shall the Party engaging in such activities/ transactions be solely responsible / liable for any action taken by any Government or regulatory authority.

11.5. Within seven (7) days of termination in any manner as contemplated in this Clause 13, all dues payable to Khosla Labs Private Limited shall be settled.

12. **WAIVERS**

No waiver by either Party of any of their terms hereof or of any breach thereof shall constitute or be deemed to be a waiver of any such terms or of any breach in any other case whether prior or subsequent thereto.

13. **FORCE MAJEURE:**

Neither Party to this Agreement shall be responsible for any delay in the performance of any terms and conditions hereunder to the extent that such delay is caused by war, revolution, riot, act of public enemy, terrorism, sabotage, epidemic, quarantine restrictions, accident, fire flood, tempest, earthquake, civil commotion, governmental action, Acts of God (Force Majeure) including, but not restricted to, strike, lock-out, fire, break-down, war, destruction of network, web space or website by way of hacking, virus prone, defacement, stoppage of display or Regulation, or restriction of Government, inability to secure Government authorization, or approval, or any other cause beyond their reasonable control.

If at any time during the term of this Agreement the performance in whole or in part by any one of the Parties, of any obligation under this Agreement is prevented or delayed by reason of war, revolution, riot, act of public enemy, terrorism, sabotage, epidemic, quarantine restrictions, accident, fire flood, tempest, earthquake, civil commotion, governmental action or Act of God the other Party shall not be entitled to terminate this Agreement neither shall any Party have any claim for damages against the other in respect of such non-performance or delay in performance, provided notice of the happening of any such event/s is given by the affected Party to the other within twenty one (21) days from the date of occurrence thereof.

14. **NOTICE**

All notices or other communications required to be given hereunder shall be in writing and delivered either personally or by registered A.D. and /or mail, certified, return receipt requested postage prepaid, and addressed as provided in this Agreement or as otherwise requested by the receiving Party. Notices delivered personally shall be effective upon delivery and notices delivered by mail shall be effective upon their

receipt by the Party to whom it is addressed. The Parties shall notify any change in address to the other Party promptly. In case of failure to intimate the other Party about the change of address, the notice shall be served to the address mentioned in this Agreement and shall be treated as properly served.

15. **ENTIRE AGREEMENT**

    This Agreement including all annexures, attachments, addendums and schedules to this Agreement constitute the entire Agreement between Khosla Labs Private Limited and the Sub-AUA pertaining to the subject matter hereof and supersedes in their entirety all written or oral agreements between the Parties.

16. **RELATIONSHIP BETWEEN PARTIES**

    The Parties to this Agreement are independent contractors and nothing in this Agreement shall make them joint ventures, partners, employees, associates, affiliates or other representatives of the other Party hereto.

17. **SEVERABILITY**

    If any provision of this Agreement is determined to be unenforceable for any reason, then the remaining provisions hereof shall remain unaffected and in full force and effect.

18. **VARIATIONS OF AGREEMENT**

    No variation or amendment to this Agreement shall bind either Party unless made in writing by the duly authorized persons/officers of both the Parties.

19. **GOVERNING LAW AND JURISDICTION:**

    It is mutually agreed between the Parties hereto that this Agreement shall be construed according to the laws of the Republic of India, and any dispute or claim arising under this Agreement shall be subject to the exclusive jurisdiction of the Courts at Bangalore.

IN WITNESS WHEREOF, the Parties have set their hands hereunto this day and date first herein above written.

For and on behalf of   For and on behalf of
Khosla Labs Private Limited   **Tamilraja**

_____   _____
Authorised Signatory   **Authorised Signatory**

ANNEXURE A

Services to be availed of and the purposes for which such services shall be used
Banking and Finance

ANNEXURE B

Fee Structure

1. One-time integration fee of Rs.5000.00 plus applicable taxes

2. Per transaction cost as per below with a minimum monthly billing of Rs.0.00:

Aadhaar non-biometric authentication (demographic, OTP)	Rs.0.00
Aadhaar biometric authentication	Rs.0.00

ANNEXURE C

The sample format for consent of authentication is as below:

Consent for Authentication

I, the holder of Aadhaar number **"xxxxxxxxxxx"**,hereby give my consent to **"Name of the Requesting Entity"** to obtain my Aadhaar number, Name and Fingerprint/Iris for authentication with UIDAI. **"Name of the Requesting Entity"** has informed me that my identity information would only be used for **"purpose"** and also informed that my biometrics will not be stored/shared and will be submitted to CIDR only for the purpose of authentication.

Signature of Aadhaar Number Holder   I agree

_____   _____