

UIDAI had published the draft Aadhaar (Authentication and Offline Verification) Regulations, 2021 on UIDAI website on 21.05.2021 for a month inviting comments and feedback. UIDAI has received various comments (mentioned below) on the draft Aadhaar (Authentication and Offline Verification) Regulations, 2021.

UIDAI is inviting further suggestions / comments on the feedback received as given below in the prescribed format by 25.08.2021. UIDAI will consider comments given only in the prescribed format.

It is further mentioned that the comments are to be sent on email ID: auth.regulations@uidai.net.in

S.No.	Regulation Number	Regulation Description	Comments of the Entity / Individual	Reason / explanation for the suggestion given	Name of the Entity / Individual

S. No.	Regulation Number	Description of the Draft Regulation	Public Comments
1	1 (2)	These regulations shall come into force on the date of their publication in the Official Gazette.	We request for a timeframe for implementation of the Regulations viz 6 months from date of publication in official Gazette
2	2 Definitions	Definitions	Need to define child and guardian in the definition clause since in clause 5 it states information to Aadhar holder wherein, in case of child inform the parent or the guardian.
3	2 (1) (aa)	“Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3 of Aadhaar Act, and includes any alternative virtual identity generated under sub-section (4) of that section;	Would this cover UID token and ANCS Token as well?
4	2 (1) (ba) 'Aadhaar Number Capture Service Token' or 'ANCS Token' 2 (1) (oc) 'UID Token' 2 (1) (od) 'Virtual ID'	<p>Aadhaar Number Capture Service Token or ANCS Token means an encrypted Aadhaar number generated for an Aadhaar number by the Authority for completion of an authentication transaction. ANCS Token shall be valid for a short period of time as prescribed by the Authority.</p> <p>UID Token means a 72-character alphanumeric string generated by the Authority mapped to the Aadhaar number and specific to a requesting entity.</p> <p>Virtual ID means an interchangeable 16-digit random number mapped with the Aadhaar number of the Aadhaar number holder.</p>	<p>While details of VID have been provided, the details and specification for ANCS and UID are not covered in the Draft Regulations.</p> <p>UIDAI needs to publish the Techal Specifications of ANCS.</p> <p>In which scenarios, ANCS token would be used. Would this lead to API specification updates as well?</p>

5	2 (1) (c) 'Authentication'	Authentication' means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.	We understand that the term 'authentication' includes both (a) Yes/No Authentication, and (b) eKYC Authentication. We request UIDAI to add these references to the definition to avoid any ambiguity.
6	2 (1) (o) 'Requesting entity' 2 (1) (oa) 'Sub-AUA' 2 (1) (ob) 'Sub-KUA'	Requesting entity' means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication.	We understand that AUAs and KUAs are 'requesting entities', and all obligations applicable to 'requesting entities' are applicable to AUAs and KUAs. However, sub-AUAs and sub-KUAs are one-level below AUAs and KUAs, and do not qualify as 'requesting entities', and are required to tie up with KUAs/AUAs. AUAs and KUAs are 'requesting entities', and all references to 'requesting entities' in the Draft Regulations are applicable to AUAs and KUAs. Sub-AUAs and sub-KUAs are in turn required to enter into arrangements with such AUAs/KUAs (i.e. requesting entities). Basis this understanding we suggest the below edits (in blue): 2 (oa) 'Sub-AUA': "Sub-AUA" means an requesting entity that uses the Yes/ No authentication facility provided by the Authority through an existing AUA. 2 (ob) 'Sub-KUA': "Sub-KUA" means an requesting entity that uses e-KYC authentication facility provided by the Authority through an existing KUA.
7	2 (2)	Words and expressions used and not defined in these regulations shall have the meaning assigned thereto under the Act or under the rules or regulations made there under or under the Information Technology Act 2000.	Please rectify the typographical and grammatical errors such as 'thereto under', 'Actor' and 'there under'

8	3A Types of Offline Verification	<p>The entities which are not allowed to collect or store the Aadhaar number shall ensure that the first 8 digits of the Aadhaar number are redacted or blacked out through appropriate means in all of the entities' records before storing the physical copies.</p>	<p>While the draft regulation provides for redaction of Aadhaar/VID No. on the physical copies however this requirement should be enforced prospectively. Further, for a scanned copy of the Aadhaar what is the treatment in case the Aadhaar/VID No. is not redacted on such scanned image. Also in case the customer provides the scanned image of the Aadhaar Card without redating the Aadhaar/VID No. should we accept such document and later redact the Aadhaar/VID No.</p> <p>Although, we understand the measures put forward by Authority to safeguard against any misuse of information collected or stored, but we wish to submit the following;</p> <ol style="list-style-type: none"> 1. Regulated entities (like TSP's/Bank's) which are currently using the different identities including Aadhaar for offline verification and taking all the security measures to safeguard the customer information including the physical copies of the POI/POA in compliance to Government bodies (like DoT/RBI) & Information technology Act. Authority should add provisions in the regulations for exempting such regulated verifying body / entities. 2. Apart for the huge impact on the current operations, it may also contradict with the existing instructions/license conditions issued by existing governing bodies, which we being a licensor needs to comply in totality. Hence we request Authority to provide sufficient time for implementation. 3. We further understand that any such changes proposed by the Authority will be applicable prospectively only.
---	----------------------------------	---	---

<p>9</p>	<p>3A (1) Types of Offline Verification</p>	<p>There shall be following types of Offline Verification services provided by the Authority, namely—</p> <p>(i) QR Code verification, which may be carried out as per the specifications given by the Authority from time to time;</p> <p>(ii) Aadhaar Paperless Offline e-KYC verification, which may be carried out as per the specifications given by the Authority from time to time;</p> <p>(iii) e-Aadhaar verification, which may be carried out as per the specifications given by the Authority from time to time; and</p> <p>(iv) Offline Paper based verification, which may be carried out by the entity. It shall be the responsibility of the concerned entity to verify the genuineness of copy of the Aadhaar letter submitted by the resident. <u>Entity shall obtain the consent of the Aadhaar number holder on the paper copy submitted by the resident.</u></p> <p>(v) Any other type of Offline verification introduced by the Authority from time to time. Further, the entities which are not allowed to collect or store the Aadhaar number shall ensure that the first 8 digits of the Aadhaar number are redacted or blacked out through appropriate means in all of the entities' records before storing the physical copies.</p>	<p>The specifications for the 4 types of offline verification services named in the Draft Regulations have not been prescribed. It would be helpful if these could be specified in the Draft Regulations itself.</p> <p>Further, the Draft Regulations does not provide details or specifications in relation to ' e-Aadhaar verification'.</p> <p>The last line of the clause 3A(1)(iv) should be modified as hereunder: Entity shall obtain the consent of the Aadhaar number holder for the paper copy submitted by the resident in either electro or physical form.</p> <p>Existence practice of Offline KYC with OTP to be discontinued.</p> <p>Comments for Clause 3A (2) Regulations need to elaborate in which scenarios will the RE have QR code</p>
<p>10</p>	<p>3A (2) - Types of offline verifications</p>	<p>The Authority shall provide various means to download QR Code, e-Aadhaar or Aadhaar Paperless Offline e-KYC.</p>	<p>We request the Authority to kindly share detail process of Authentication via QR Code to enable us to examine the techal architecture to be followed for the activation process at our end. We also understand that currently authentication through QR code does not share/provide the demographic biometric details of Aadhaar holder, which may lead to the issues related customer verification.</p>

11	4 (2) (b)	A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.	UIDAI to clarify on number of attempts allowed & OTP validity.
12	4 (3) Modes of Authentication	A requesting entity may choose suitable mode(s) of authentication from the modes specified in sub-regulation (2) for a particular service or business function as per its requirement, including multiple factor authentication for enhancing security. For the avoidance of doubt, it is clarified that e-KYC authentication shall only be carried out using OTP and/ or biometric authentication	<p>Under the RBI issued Master Directions on the Issuance and Operation of Prepaid Payment Instruments (PPI), an issuer of PPIs is required to collect the officially valid document (OVD) ID number of customers to be able to open a minimum details wallet for customers (ie. Upto INR 10,000 limit). While the definition of OVD includes Aadhaar, given the restriction on storage of Aadhaar number, we are unable to offer customers this option, despite most customers wanting to submit Aadhaar number for such purposes.</p> <p>We therefore request UIDAI to clarify if the Aadhaar number / VID can be collected and stored by the PPI issuer for KYC for the minimum KYC PPIs that it issues.</p> <p>It has been stated that the requesting entity can choose the mode of authentication, further clarification/ elaboration on the same is required under the regulations.</p>
13	4A (3) Virtual Identity number (VID)	The Aadhaar number holder may use VID in lieu of Aadhaar number for 'online authentication' or e-KYC.	<p>The use of the undefined term 'online authentication' is not clear.</p> <p>Also, we require clarity on the instances where VID is permitted to be used in place of Aadhaar number.</p> <p>We request UIDAI to clarify that the VID can be used at all instances and for all purposes as the Aadhaar number. We also request UIDAI to clarify the meaning of the term 'online authentication'.</p> <p>We request UIDAI to clarify that the VID can be used at all instances and for all purposes as the Aadhaar number. We also request UIDAI to clarify the meaning of the term 'online authentication'. Further, the ASA/ AUA should make necessary infrastructural changes made available to accept VID in lieu of Aadhaar number since the length of the VID is 16-digit whereas that of Aadhaar is 12 digits.</p>

14	5 (1) - Parent Consent	At the time of authentication or Offline Verification, a requesting entity or Offline Verification Seeking Entity (OVSE) shall inform the Aadhaar number holder i.e. in case of a child, inform the parent or guardian	<p>What is the age to be considered for a person to fall under the child category.</p> <ul style="list-style-type: none"> • To generate xml file, in what situation Clause 5 of the draft regulations will be applicable? • ‘what is verification’? • What is the difference between Authentication and Offline verification? <p>These things are already part of the consent and final display of authentication like in case of attendance App Marking of attendance is displayed—making too much to sub-aau/aau App will ask for further changes in App and financial implication like in case of SMS.</p>
15	5 (2) Information to the Aadhaar number holder	A requesting entity shall ensure that the information referred to in sub-regulation (1) above is provided to the Aadhaar number holder in local language as well.	<p>Applicable for authentication & offline verification. It would be an operational challenge to determine the local language for a user.</p> <p>We request UIDAI to modify the provision to not make it mandatory. It can be proposed that the requesting entities make this available to the customers, preferably in English, Hindi and the local language.</p> <p>The said sub-regulation should be modified as under: “A requesting entity shall ensure that the information referred to in sub-regulation (1) above is provided to the Aadhaar number holder in local language as well where such Aadhaar number holder is unable to communicate in English.”</p> <p>Offline Verification is generally used by banks and NBFCs as part of loan offerings through digital modes and their apps or websites are in English. All the documents are executed in English language except where the customer expresses inability to read and understand English. Hence, we recommend that local language should be made applicable only in cases where it is determined that such person is unable to understand in English language.</p> <p>Department of Telecommunication (DoT), already specified means to communicate the details to the subscriber including providing the details in regional language. In case agencies already providing details in compliance to the existing instruction issued by their governing bodies same may be exempted from such compliances.</p> <p>Providing such details in local language during processing (in App) is not technically feasible for PAN-India operators, as this will require complete redevelopment to support all the regional languages.</p>

16	5 (3)	A requesting entity shall ensure that the no service is denied to any resident for refusing to or being unable to undergo authentication and or offline verification provided that the resident is able to identify himself through a viable alternative means as suggested by the requesting entity under sub-regulation (1) (c) above.	<p>1. Aadhar should allow linking of more than one phone number (classified as primary and secondary) with one profile or identity.</p> <p>2. Alternate process for OTP verification like</p> <p>a) Click on link received via sms to authenticate or confirm request</p> <p>b) Receive OTP via IVR (voice enabled)</p> <p>c) QR code based</p>
17	6 Consent of the Aadhaar number holder - Need Discussion	<p>(1) After communicating the information in accordance with Regulation 5, a requesting entity or Offline Verification Seeking Entity (OVSE) shall obtain the consent of the Aadhaar number holder or in case of a child, the consent of the parent or guardian of the child for the authentication or verification.</p> <p>(2) A requesting entity or OVSE shall obtain the consent referred to in sub-regulation (1) above in physical or preferably in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.</p> <p>(3) A requesting entity shall provide the facility to withdraw consent by the resident. In case a resident withdraws his/her consent or in case of a child, by the parent or guardian, the resident's Aadhaar data shall be deleted by the requesting entity in a verifiable manner and an acknowledgement of the same to be provided to the resident. If resident wishes to continue with the service, requesting entity shall provide alternate means of identity verification.</p>	<p>A user's consent is obtained by the 'regulated entity' under the KYC framework of the RBI and not by the requesting entity (or sub-AUA or sub-KUA). Onus to prove whether consent has been obtained or not and the details / logs of the consent, must be with the 'regulated entity'.</p> <p>We understand the position of deletion of Aadhaar data once the user withdraws consent, it is important to have an exception to this position that permits record keeping for regulatory reasons. Avoid any conflict of the Draft Regulations with the other RBI requirements that mandate storage of data/ records.</p> <p>It is important to recognise that the service to the customer can be stopped until customer completes KYC through alternative means.</p> <p>We propose to remove the phrase "in the manner and form as may be specified by the Authority for this purpose". In the event a particular mechanism is proposed, please consider including it in the Draft Regulations.</p> <p>We have proposed an alternate to clause (3) in view of the comments, where the revisions are provided in red:</p> <p>"(3) A requesting entity shall provide the facility to withdraw consent by the resident. In case a resident withdraws his/her consent or in case of a child, by the parent or guardian, the resident's Aadhaar data shall be deleted by the requesting entity in a verifiable manner and an acknowledgement of the same to the resident, provided however that requesting entity may retain or be permitted to retain the Aadhaar data in accordance with the requirement under applicable law and for compliance with orders of regulators or government agencies. If resident wishes to continue with the service, requesting entity shall provide alternate means of identity verification, and the requesting entity may suspend the service to the customer until the customer verifies identity through alternate means of provides consent under sub-regulation (1) above."</p>

<p>6 Consent of the Aadhaar number holder - Need Discussion</p>		<p>Comments for Clause 6 (3) Revoking consent is like saying I have changed my mind now, hence for real-time services, this should not be applicable. It is important to note that any entity using Aadhaar for on-boarding or providing services has gone through compliant process allowed under the law allowed, incurred some cost and customer has given explicit consent (as is mandated by law). E.g. if customer opens a bank account, uses it for some time and then decides to revoke consent or uses SIM card issued through eKYC, commits fraud/crime and then revokes consent after years, it would not help. This does not seem to be logical for services which are part of essential services and have national security implications</p> <p>Comments for Clause 6 (3) Should not allow withdraw of consent as there is no risk for a customer. This will pose a challenge to the Regulated Entities, e.g. as per PMLA & RBI directions a KYC is valid for the tenure of the relationship and 5 years after the cessation of the relationship, Such Regulated Entities are required to keep documentation for 5 years after the cessation of the customer account. If we delete such documents and trail, the history POI & POA history cannot be traced and can lead to potential frauds and other audit issues where the trail cannot be established.</p>
<p>6 Consent of the Aadhaar number holder - Need Discussion</p>		<p>Allow holders to delegate consent to a person who can verify the identity for the service offered.Needs to be discussed</p> <p>Comments on Clause 6 (2) 1. Consent should be extended to onboard other products offered by HFC 2. Updated KYC info – company should be allowed to request updated information of the customer automatically at defined intervals or till such time customer account is active.</p> <p>Comments on Clause 6 (3) 1. Clarity should be given in the regulations, at what point of time/ scenarios can the resident withdraw the consent? 2. Suggestion to revisit this clause, since this data is used by the financial institution for KYC purposes. Further as per RBI’s record retention policy, this data has to be maintained in accordance with the law.</p>

	6 Consent of the Aadhaar number holder - Need Discussion	<p>Clause 6 (3)</p> <p>Withdrawal of consent and consequent deletion of Aadhaar data may also impact the accrued rights and obligations of the parties, including performance of contractual obligations including pending payment obligations, for which a reasonable period of retention of certain identity and commutation information pertaining to the resident may become necessary. In addition, for regulated entities backed by law such as telecommutation service providers and banking entities, the licensor also stipulates a minimum periods of retention of such information. We request the Authority to consider enabling the following carve-out to accommodate such retention:</p> <p>“A requesting entity shall provide the facility to withdraw consent by the resident. In case a resident withdraws his/her consent or in case of a child, by the parent or guardian, the resident’s Aadhaar data shall be deleted by the requesting entity, subject to fulfilment of all applicable legal, contractual and regulatory obligations of the requesting entity and the resident, in a verifiable manner and an acknowledgement of the same to the resident shall be provided., If resident wishes to continue with the service, requesting entity shall provide alternate means of identity verification.”</p> <p>Further, in consequent to the existing regulatory mandates & based on the system and process deployed by entities, it’s not feasible to provide continuity of the services once resident/subscriber wishes to withdraw consent, hence necessary proviso to be added to the stipulated regulation or may be removed.</p>
--	---	---

	6 Consent of the Aadhaar number holder - Need Discussion	<p>Regulated entities have certain obligations to meet in terms of record keeping, irrespective of a customer's desire to withdraw intent to use Aadhaar. Also, the consent obligation should be imposed on the regulated entity, to be determined by it as per the process flow/ systems. We have proposed an alternate to clause (2) and (3) accordingly (in blue):</p> <p>"(2) A requesting entity or OVSE shall obtain the consent referred to in sub-regulation (1) above in physical or preferably in electro form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.</p> <p>(3) A requesting entity shall provide the facility to withdraw consent by the resident. In case a resident withdraws his/her consent or in case of a child, by the parent or guardian, the resident's Aadhaar data shall be deleted by the requesting entity in a verifiable manner and an acknowledgement of the same to the resident, provided however that requesting entity may retain or be permitted to retain the Aadhaar data in accordance with the requirement under applicable law and for compliance with orders of regulators or government agencies. If resident wishes to continue with the service, requesting entity shall provide alternate means of identity verification, and the requesting entity may suspend the service to the customer until the customer verifies identity through alternate means of provides consent under sub-regulation (1) above. Additionally, the resident shall be made aware on a set frequency (not more than 3 months) by means of an email notification / SMS hyperlink about the list of OVSEs to which the resident has offered his consent in the past 3 months. Also, the notification shall carry the facility to withdraw the consent within a specified timeframe.</p>
--	---	--

18	7. Capturing of biometric information by requesting entity	<p>(1) A requesting entity shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by the Authority.</p> <p>(1a) All biometric devices used for authentication shall be Registered Devices as per the standards specified by the Authority from time to time.</p> <p>(1b) All the biometric devices shall be registered with the server of the requesting entity.</p> <p>(2) A requesting entity shall necessarily encrypt and secure the biometric data at the time of capture as per the specifications laid down by the Authority.</p> <p>(3) For optimum results in capturing of biometric information, a requesting entity shall adopt the processes as may be specified by the Authority from time to time for this purpose.</p>	<p>'certified biometric device' has not been defined. The Draft Regulations rather defines the term 'Registered Device' which has been used in context of biometric devices used for authentication. UIDAI is requested to provide clarity in the Draft Regulations.</p> <p>Also, we request UIDAI the ensure that each device does not require registration for use for biometric information, and a one-time registration should be sufficient, if UIDAI proposes of have any registration requirement.</p> <p>Comments for clause 7(1)(b)</p> <p>As of today, for all OFFUS transactions, the Biometric Device ID is sent along with the Issuer Bank's AUA Code and License Key. The Biometric Device ID, is registered with the Acquirer Bank. This clause may be suitably changed to incorporate this reality or an additional clarification specific to AEPS transaction may be released to define & identify the requesting entity as Acquirer bank and not as Issuer Bank.</p> <p>Comments for clause 7(1)(b)</p> <p>Clarification sought on the exact meaning 'server of the RE'.</p> <p>Comments for clause 7(1)(b)</p> <p>needs to be elaboatred with example</p> <p>Clause 7(1)(2)</p> <p>what is the need of this point when RD is present.</p>
19	8(1)	<p>8. Devices, client applications, etc. used in authentication.—</p> <p>(1) All devices and equipment used for authentication shall be certified as required and as per the specifications issued, by the Authority from time to time for this purpose.</p>	<p style="text-align: center;">What about face authentication?</p>

20	9 (1) (2) (4)	<p>9. Process of sending authentication requests.—</p> <p>(1) After collecting the Aadhaar number or any other identifier provided by the requesting entity which is mapped to Aadhaar number and necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application shall immediately package and encrypt these input parameters into PID block before any transmission, as per the specifications laid down by the Authority, and shall send it to server of the requesting entity using secure protocols as may be laid down by the Authority for this purpose.</p> <p>(2) After validation, the server of a requesting entity shall pass the authentication request to the CIDR, through the server of the Authentication Service Agency as per the specifications laid down by the Authority. The authentication request shall be digitally signed by the requesting entity and/or by the Authentication Service Agency, as per the mutual agreement between them.</p> <p>(4) In all modes of authentication, the Aadhaar number is mandatory and is submitted along with the input parameters specified in sub-regulation (1) above such that authentication is always</p>	<p>(1) identifier means UID token ?</p> <p>(2) why validation is written normally these are the part of workflow of application so what else is required ?</p> <p>4) why Aadhaar number is mandatory written ?</p>
21	10	(1) The Aadhaar number holder shall be notified by the requesting entity about any authentication,	The Draft Regulations envisage a shift of the notification obligation from UIDAI (under the current regulations) to requesting entity. While the obligation to notify the user is reasonable, the

		<p>(1) The Aadhaar number holder shall be notified by the requesting entity about any authentication, through email and/or SMS on mobile number and/or paper-based acknowledgement about success or failure of authentication on each request. Such notification/acknowledgement shall include entity's name, date and time of authentication, auth response code, last 4 digits of Aadhaar number and purpose of authentication, as the case may be.</p> <p>(3) In case of authentication failure the requesting entity should, in clear and precise language, inform the resident about the reasons of authentication failure such as Suspended/Cancelled Aadhaar or Biometric/Aadhaar Locking.</p>	<p>It is submitted that in compliance to the existing instructions for verification issued from the telecommuamtion governing body i.e. Department of Telecommuamtion (DoT), which already mandates to commuate the verification status details (success or failure) to the subscriber both during and post verification. Hence we submit to Authority that in case verifying agencies already providing details to the customer in compliance to the existing mandates issued by their governing bodies then same may be exempted from such duplicate compliances of providing details to the subscriber at each and every authentication through email/SMS/paper based, as this will have a huge impact on our systems and process which needs to be completely redeveloped.</p> <p>Modify this provision to allow other electro modes, including mobile based push notifications, commuation to the customer on the App as part of the process flow, or any other mobile application based mechanism.</p> <p>Also, we understand that such commuation to customer may be undertaken either by the requesting entity, or the Sub-KUA, Sub-AUA if contractually authorised by the requesting entity (to avoid duplication of commuation to the customer from multiple entities). Please confirm.</p> <ul style="list-style-type: none"> • The Aadhaar holder should be able to retrieve this information in the future using the request Id or unique identifier (customer number) of the requesting entity. • The holder should also receive the information about removing the consent and alternative means of identity verification. • Purpose of authentication should contain the service provided/offered information instead of just saying identity verification.
22	10 (2)	<p>(2) The Aadhaar number holder shall be notified by the OVSE about any offline verification, through email and/or mobile number and/or paper based acknowledgement about success or failure of offline verification on each request.</p>	<p>Under the said clause OSVE needs to notify Aadhar number holder about any offline verification. While this may be fine for QR code verification but for the paperless mode this is initiated by the Aadhar number holder itself. Operationally may not be feasible.</p>
23	11- Aadhaar / Biometric Locking/Unlocking	<p>The Authority may enable an Aadhaar number holder to lock and Unlock his Aadhaar number.</p>	<p>Require awareness about how to temporally lock his/her Aadhaar number / biometrical records temporary and permanently. The process of locking / unlocking of biometric / Aadhaar should made be available</p> <p>Process and/or platform for the locking/unlocking of Biometric information is not clear. Elaborated process should be included.</p>

24	11A.Aadhaar locking	(3) In case of a locked Aadhaar, the Authority will allow the resident to authenticate using Virtual ID or other means.	We believe that the reference to 'Aadhar' does in fact refer to 'Aadhaar number'. UIDAI to clarify the correct terminology. Suggested revised clause: “In case of a locked Aadhaar number, the Authority will allow the resident to authenticate using Virtual ID or other means.”
25	12. Appointment of Requesting Entities and Authentication Service Agencies	<p>(1) Agencies seeking to become requesting entities to use the authentication facility provided by the Authority shall apply for appointment as requesting entities in accordance with the procedure as may be specified by the Authority for this purpose from time to time. Only those entities that fulfil the criteria laid down in Schedule A are eligible to apply. The Authority may by order, amend Schedule A from time to time so as to modify the eligibility criteria.</p> <p>(1A) Requesting entity and ASA shall meet technical and security criteria as specified by the Authority from time to time.</p>	This provision lists out the obligations applicable to a requesting entity, including the obligation to obtain authorisation / permission. We believe that the obligations provided here are only applicable to AUA and KUA, and not sub-AUA or sub-KUA, as Sub-KUAs/ Sub-AUAs are required to have arrangements with the KUA/AUA. We request UIDAI to confirm on the position mentioned here.
		(10) The Authority may from time to time, determine if requesting entities will be allowed to perform authentication using Aadhaar number or Virtual ID or UID Token or ANCS or any other identifier.	<p>We recommend that the determination must be registration-specific and be commuted by the UIDAI along with confirming the application. In case of subsequent changes to this, the requesting entity will need to make substantial changes to the integrations/ processes, and having this clarity upfront will help the entity build the appropriate controls. We request UIDAI to consider removing this provision.</p> <p>We request UIDAI to consider removing this provision as the requesting entities will comply with the provisions and specification by UIDAI at the time of application approval.</p>

27	13	<p>Procedure where application for appointment is not approved. —</p> <p>(1) In the event an application for appointment of requesting entity, Authentication Service Agency, as the case may be, does not satisfy the requirements specified by the Authority, the Authority may reject the application.</p> <p>(2) The decision of the Authority to reject the application shall be communicated to the applicant in writing within thirty days of such decision, stating therein the grounds on which the application has been rejected.</p> <p>(3) Any applicant, aggrieved by the decision of the Authority, may apply to the Authority, within a period of thirty days from the date of receipt of such intimation for reconsideration of its decision.</p> <p>(4) The Authority shall reconsider an application made by the applicant and communicate its decision thereon, as soon as possible in writing.</p>	<p>Addition should be made saying that the decision of the Authority after the application of reconsideration of its decision should be made final and no appeal/reapplication can be allowed. It will help with the hearing same application again and again, only because the applicant is not satisfied with the decision.</p>
28	14 (1) (ca)	<p>ensure that the Aadhaar number/Virtual ID/ANCS Token provided by the resident for authentication request shall not be retained by the device operator or within the device or at the AUA server(s);</p>	<p>device operator – how to do this ?</p>
29	14 (1) (ga)	<p>A requesting entity shall have the following functions and obligations:</p> <p>(ga) obtain approval from the Authority before appointing any third party entity as Sub-AUA/Sub-KUA.</p>	<p>The Sub-KUA entity approved by the Authority should be considered as entity notified under first proviso to sub-section (1) of section 11A of the PML Act.</p> <p>Already a letter written to UIDAI regarding approval process and responsibility of AUA – not practical for AUA like – issue raised by DG to CEO .</p>

30	14 (1) (h)	ensure that its operations and systems are audited by information systems auditor certified by a recognised body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;	audit should be for at least 2 years, one year is too less This provision seems contracting to #20 above which mentions log storage duration as 2 years.
31	14 (1) (j) - Fraud Analysis	The requesting entity shall in case of any investigation involving authentication related fraud(s) or dispute(s), it shall extend full cooperation to the Authority, or any agency appointed or authorised by it or any other authorised investigation agency	We as TSP have our own internal checks and balances in compliance to DoT's License agreement / Guidelines/ instructions issued by them time to time including identification of individual subscribers having more than 9 connections and taking necessary actions thereof. We request the Authority to kindly let us know what the additional checks are and balances are required from us to comply with / perform along with the reporting process (if any).
32	14. Roles and responsibilities of requesting entities	(1) A requesting entity shall have the following functions and obligations: - (k) in the event the requesting entity seeks to integrate its Aadhaar authentication system with its local authentication system, such integration shall be carried out in compliance with standards and specifications issued by the Authority from time to time.	The use of the term 'local authentication system' is unclear. We request UIDAI to clarify the integration and the systems mentioned in this clause. Also, UIDAI is requested to clarify the meaning of the term 'local authentication system' and permissible use cases of the same. UIDAI is requested to clarify the meaning of the term 'local authentication system' and permissible use cases of the same.

33	14 (1) (ma)	<p>REs may now charge a fee for authentication services</p> <p>14. Roles and responsibilities of requesting entities. —</p> <p>(1) A requesting entity shall have the following functions and obligations:—</p> <p>(ma) may agree upon the authentication charges for providing authentication services to its customer, with such customer, and the Authority shall have no say in this respect, for the time being; however, the Authority’s right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;</p>	<ul style="list-style-type: none">• The second part of the provision is unclear. It appears to convey the opposite of its intention. In its current form, UIDAI has no power to intervene. The provision has been redrafted (column 4 and 5).
----	-------------	---	---

34	14 (1) (mb) - Redacting of Aadhaar Number	Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters shall be masked by the requesting entity by redacting the first 8 digits of the Aadhaar number before storing the physical copies.	<p>We as TSPs acquire the customer through the DoT's approved Paper base/DKYC/EKYC processes. When the customer brings the Aadhaar in physical form / photocopy it is not at all possible to redact the Aadhaar number on Physical form. Even if customer himself/herself comes up with blacked out Aadhaar number (only last 4 digits are visible) in that case the d-duping of the customer within our existing subscriber database will not be possible and may lead to security / compliance issues with regard to the guidelines / instructions issued by DoT for subscriber verifications from time to time.</p> <p>This clause needs to be deliberated along with Department of Telecommuation (DoT)</p> <p>what about school and other organisation who are not part of requesting entity ? practically followed by entity ?</p> <p>We understand the measures to safeguard against any misuse of information collected or stored, but we wish to submit the following;</p> <ol style="list-style-type: none"> 1. Regulated entities (like TSP's/Bank's) are using different identities including Aadhaar for offline verification and already taking all the security measures to safeguard the customer information including the physical copies of the POI/POA in compliance the license conditions by DoT/RBI & Information technology Act. Authority should add provisions in the regulations for exempting such regulated verifying body / entities. 2. huge impact on the current operations and it may also contradict with the existing instructions/license conditions issued by existing governing bodies, which we being a licensor needs to comply in totality. Request Authority to provide sufficient time for implementation 3. We further understand that any such changes proposed by the Authority will be applicable prospectively only.
35	14 (1) (o)	(o) shall take specific permission of the Authority and sign appropriate agreement with the Authority, if requiring storage of Aadhaar number for non-authentication purposes. Aadhaar number shall be stored in a secure manner as specified by the Authority from time to time	<p>is it to be done Authentication application also? what bout organizations who are not requesting entity?</p> <ul style="list-style-type: none"> • It is unclear what non-authentication purpose refers to in this case. Given that storage of Aadhaar numbers by requesting entities is done with the consent of the Aadhaar number holder, the role of UIDAI should be limited to laying down some basic safeguards and security protocols. • Separate permission from UIDAI not required by law. Redrafted provision (column 4 and 5)

36	14A. Obligations of Offline Verification Seeking Entities:	Obligations of Offline Verification Seeking Entities	<p>(i) We request for more clarifications on compliance expectations for OVSEs</p> <p>(ii) We request for Per Unit charges for KYC by OVSE's</p> <p>(iii) We request clarifications in respect to whether KUA/AUA require separate license for becoming OVSE ?</p> <p>We request that once the fraud is established and the data is published by the concerned OVSE, the UIDAI should also have an SOP for the course of action on the compromised data.</p>
37	14A. Obligations of Offline Verification Seeking Entities:	14A(1)(b) shall not collect, use or store Aadhaar number or biometric information of any individual for any purpose or share offline Aadhaar data with any other entity except in accordance with the Act and Regulations framed thereunder;	<p>The following proviso to be included after Regulation 14A(1)(b):</p> <p>Provided that receipt of Aadhaar number from an individual by an OVSE for the purpose of Offline Verification shall not be deemed to be collection, usage or storage by such OVSE.</p> <p>Provided further that the offline Aadhaar data may be shared by the OVSE with any other entity as required to comply with any applicable law or regulations.</p> <p>The rationale for the recommendation is as under:</p> <p>a. Addition of the first proviso is recommended to clarify that receipt of Aadhaar number solely for the purpose of conducting Offline Verification will not tantamount to collection, usage or storage by such OVSE. The Aadhaar number would be received only for the purpose of Offline Verification and once the process is complete, the same will be deleted from the records of the OVSE.</p> <p>b. In terms of the PMLA, Banks, Non-Banking Finance Companies (“NBFCs”) and Housing Finance Companies (“HFCs”) (collectively referred as “Regulated Entities”) regulated by the Reserve Bank of India, are required to submit the KYC details of the customer to the Central Know Your Customer Registry (“CKYCR”). Accordingly, the Regulated Entities are mandatorily required to share the information collected under Offline Verification with CKYCR.</p> <p>c. The PMLA & Rules also require the Regulated Entities to make available the identification records and transaction data to the competent authorities upon request.</p> <p>d. For verifying the identity of customers, the KYC Master Directions allow Regulated Entities to rely on the due diligence done by a third party which requires sharing of KYC information between the third party and the Regulated Entities.</p>

<p>38</p>	<p>15 (1) & (2) 16 (1) & (2)</p>	<p>15 (1) A requesting entity may use Yes/ No authentication facility provided by the Authority for verifying the identity of an Aadhaar number holder for its own use or on behalf of other agencies.</p> <p>15 (2) A requesting entity may permit any other agency or entity to perform Yes/ No authentication by generating and sharing a separate license key for every such entity through the portal or any other mechanism provided by the Authority to the said requesting entity. For the avoidance of doubt, it is clarified that such sharing of license key is only permissible for performing Yes/ No authentication and is prohibited in case of e-KYC authentication.</p> <p>16 (1) A KUA may use the e-KYC authentication facility provided by the Authority for obtaining the e-KYC data of the Aadhaar number holder for its own purposes.</p> <p>16 (2) A KUA shall obtain specific permission from the Authority by submitting an application for sharing of e-KYC data with Sub-KUA and such data may be shared in encrypted form as per the guidelines issued by the Authority from time to time, with specific consent of Aadhaar number holder.</p>	<p>We understand that any entity (including private, unregulated entities) may approach AUAs to perform Yes/ No authentication, however, KUAs may only perform e-KYC for sub-KUA. We request UIDAI to confirm if our understanding is correct here. Further, UIDAI is requested to clarify the reference to 'agencies' in the provision 15 (1) of the Draft Regulations.</p> <p>Comments for clause 15 (2)</p> <p>Permission to give license key to other agencies by the authority should be done prior to written notice/intimation to the Authority. Proper data of entities to be maintained by the requesting agencies to whom license key has been provided. This will help in total accountability and management of information of the residents by the Authority.</p> <p>Clause 15 (1) - meaning of on behalf of other agency? Clause 15 (2) - other agency and SUB-AUA difference? legality? implementation aspect? permission from UIDAI? Clause 16 (2) - Govt sub-kua must be allowed without permission. ? sharing of data in encrypted for should be for public network .. otherwise it will put to much extra load on this and server performance of thru put of servers.? data mean what eKYC XML?</p>
<p>39</p>	<p>15 (3A)</p>	<p>(3A) AUAs/KUAs/Sub-AUAs/Sub-KUAs shall use their client application for Aadhaar authentication which shall be digitally signed by the requesting entity.</p>	<p>Digitally signed by the requesting entity is not possible for ?</p>

40	15 (5)	(5) The requesting entity shall be jointly and severally liable, along with the entity or agency with which it has shared a license key, for non-compliance with the regulations, processes, standards, guidelines and protocols of the Authority.	Not possible for
41	16 (3) 17 (1) (d)	<p>16 (3) The Sub-KUA with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall not share it further with any other entity or agency.</p> <p>17 (1) (d) A requesting entity shall ensure that identity information received during authentication is only used for the purpose specified to the Aadhaar number holder at the time of authentication, and shall not be disclosed further, except with the prior consent of the Aadhaar number holder to whom such information relates. Further:</p> <p>(i) The requesting entity may seek consent of the Aadhaar number holder to modify the Confidential Document purpose specified in the first instance.</p> <p>(ii) Consent may be withdrawn through a communication of opting out of the modified purpose as per the process prescribed by the requesting entity.</p> <p>(iii) Consent maybe presumed to be given if no communication of opting out of the modified purpose is received by requesting entity.</p> <p>Provided that the process and consequences of opting out is communicated by the requesting entity to the Aadhaar number holder in a clear, concise and timely manner before the implementation of the modified purpose.</p>	<p>In context of clause 17 (1) (d), the term 'identity information' has been defined in the Act as: "identity information in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information".</p> <p>Clause 16 (3) imposes a restriction on the sub-KUA to share the e-KYC data of the Aadhaar number holder. In our view, the sub-KUA should be permitted to share / disclose the e-KYC data with other entities, as long as the Aadhaar number holder has provided consent. We request the UIDAI to consider modifying Clause 16 (3) to even permit sub-AUAs and sub-KUAs to share or disclose identity information of the Aadhaar number holder for purposes other than authentication based on consent of such Aadhaar number holder.</p> <p>Comments for Clause 16 (3) - Revise as- "The Sub-KUA with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall not share it further with any other entity or agency except for the persons or agency employed by it for performing authentication functions."</p> <p>Comments for Clause 17 (1) (d) (iii) - Timeline should be provided within which the Aadhaar number holder has the right to withdraw the consent. Same should be mentioned in the commuation of request made to be the Aadhaar number holder for modification purposes.</p> <p>Consider modifying Clause 16 (3) to permit sub-AUAs and sub-KUAs to share or disclose identity information of the Aadhaar number holder for purposes other than authentication, with the consent of such Aadhaar number holder.</p>

42	16 (4) - Revoking of Consent	The Aadhaar number holder may, at any time, revoke consent given to a KUA/Sub-KUA for storing his e-KYC data, and upon such revocation, the KUA/Sub-KUA shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.	<p>Considering the dynamic nature of the business, the revocation of consent by the customer will lead to the multiple entries into the entire customer life cycle and will also impact on its associated services / benefits such as Credit Limit, Active VAS & Data packs etc.</p> <p>Further as the Authority is already aware that the telecom services play's an important role for National Security, we as TSP have to comply with the DoT guidelines including the periodic /monthly audits perform by Licensor wherein we need to provide the information /documents /consents given by the customer at the time of taking the connections. By allowing the customer to revoke his/her consent (deletion of records) and taking new KYC documents will create a gap / mismatch between its verification / KYC journey.</p> <p>In addition to the above it will also be difficult to produce the documents to the licensor / LEAs in case the matters is under audit / investigations. Also, in case of any compliance related issues, the same may also lead to disconnection of the services as well as customer inconvenience.</p>
43	16A (2)	No entity or person shall perform Offline Verification on behalf of another entity or person.	<p>The ability to undertake offline verification is not based on a registration. Accordingly, the same should be permitted to be outsourced to a third-party service provider.</p> <p>We request the UIDAI to modify this provision with an ability for an entity to engage a third-party service provider to perform such verification on behalf of a regulated entity.</p> <p>This will conflict with Master Directions KYC (MD KYC) Clause 14 which allows reliance on DD done by another Regulated Entity. Thus, when we take Photo, POI & POA through an OFFLINE XML documents we will not be able to rely on such document collected by another RE. In practicality the share code could have changed, more so, the sharecode is not normally stored in records.</p> <p>We request the UIDAI to modify this provision with an ability for an entity to engage a third-party service provider to perform such verification on behalf of a regulated entity.</p>

44	16A (4)	<p>The Aadhaar number holder may, at any time, revoke consent given to an OVSE for storing his/her offline Aadhaar data, and upon such revocation, the OVSE shall delete the offline Aadhaar data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.</p>	<p>Include an exception that permits record keeping for regulatory reasons. This will help avoid inconsistency between the Draft Regulations with the other RBI requirements that mandate storage of data/ records. Proposed an alternate to clause (4)</p> <p>"The Aadhaar number holder may, at any time, revoke consent given to an OVSE for storing his/her offline Aadhaar data, and upon such revocation, the OVSE shall delete the offline Aadhaar data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder, provided however that OVSE may retain or be permitted to retain the Aadhaar data in accordance with the requirement under applicable law and for compliance with orders of regulators or government agencies."</p> <p>The following proviso to be added after Regulation 16(A)(4): Provided that the OVSE shall not be required to delete such offline Aadhaar data where the OVSE is required to maintain or retain the same under any applicable law or regulation.</p> <p>The regulation should not allow withdraw of consent to the customer. As per PMLA & RBI directions a KYC is valid for the tenure of the relationship and 5 years after the cessation of the relationship. Such Regulated Entities re required to keep documentation for 5 years after the cessation of the customer account. If we delete trail, the history POI & POA history cannot be traced and can lead to potential frauds and other audit issues where the trail cannot be established.</p> <p>“A requesting entity shall provide the facility to withdraw consent by the resident. In case a resident withdraws his/her consent or in case of a child, by the parent or guardian, the resident’s Aadhaar data shall be deleted by the requesting entity, subject to fulfilment of all applicable legal, contractual and regulatory obligations of the requesting entity and the resident, in a verifiable manner and an acknowledgement of the same to the resident shall be provided., .”</p>
45	17 (1) (a)	<p>(1) A requesting entity shall ensure that: (a) the core biometric information collected from the Aadhaar number holder is not stored, shared or published for any purpose whatsoever, and no copy of the core biometric information is retained with it;</p>	<p>RD is used?</p>

46	17(1)(d)	<p>17. Obligations relating to use of identity information by requesting entity-</p> <p>(iii) Consent may be presumed to be given if no communication of opting out of the modified purpose is received by requesting entity. Provided that the process and consequences of opting out is communicated by the requesting entity to the Aadhaar number holder in a clear, concise and timely manner before the implementation of the modified purpose.</p>	<p>Consent should not be presumed for any other purpose than the original consent. Modified purposes should always require consent.</p> <ul style="list-style-type: none"> • S.29(3) of the Act must be examined carefully while framing this particular amendment. It should not be taken to mean that the purposes can only be specified once, at the time of the first authentication, and cannot be modified subsequently. • Based on the text of the provision, there is reasonable scope to argue that s.29(3) states that every time authentication is undertaken, the RE is empowered to specify purposes for which the information is being collected. • Accordingly, in a scheme where authentication is undertaken on a frequent basis, no separate power needs to be given to the RE to modify the purposes. A fresh set of purposes can be issued every time authentication is performed under the scheme. • However, in schemes with infrequent authentication, REs may have to be given the power to modify purposes. • This being said, there still continues to be a legal risk of this amendment being viewed as exceeding the scope of the Act. This caveat needs to be noted. • The redrafted provision with suitable changes is in Column 4, in addition to an amendment to the Sharing of Information Regulations, 2016, which also has a similar restriction on sharing of identity information by REs. This is subject to the caveat identified above.
47	17(1)(g)	<p>(g) all relevant laws and regulations in relation to data storage and data protection relating to the Aadhaar-based identity information in their systems, that of their agents (if applicable) and with authentication devices, are complied with.</p>	<p>Requesting entities should publish the compliance periodically as defined by the authority.</p>

<p>48</p>	<p>Storage of Aadhaar Number / VID</p> <p>4A (4), 12 (8), 14 (1)(o), 17 (1)(e), 18 (1)(b)</p>	<p>4A (4) No entity shall store Virtual ID in its system.</p> <p>12 (8) The Authority may from time to time, determine requesting entities which may be allowed to store Aadhaar number or masked Aadhaar number</p> <p>14(1)(o) shall take specific permission of the Authority and sign appropriate agreement with the Authority, if requiring storage of Aadhaar number for non-authentication purposes. Aadhaar number shall be stored in a secure manner as specified by the Authority from time to time.</p> <p>17 (1)(e) the identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected against access, use and disclosure not permitted under the Act and its regulations</p> <p>18 (1) (b) specified parameters received as authentication response including full Aadhaar number or masked Aadhaar, as the case may be.</p>	<p>There seems to be ambiguity amongst certain provisions regarding scenarios when a requesting entity may store the Aadhaar number.</p> <p>We request the UIDAI to clarify both the instances in which a requesting entity is either permitted to store Aadhaar number or prohibited from doing so to avoid any ambiguities in the future.</p> <p>We request UIDAI to define the encryption standard and the method for encryption has to be mandatorily made uniform across the board for subscriber entities.</p>
------------------	---	--	--

49	18 (1)	<p>18. Maintenance of logs by requesting entity. —</p> <p>(1) A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:—</p> <p>(a) specified parameters of authentication request submitted excluding Aadhaar number, Virtual ID, ANCS Token or UID token;</p> <p>(b) specified parameters received as authentication response including full Aadhaar number or masked Aadhaar, as the case may be;</p> <p>(c) the record of disclosure of purpose for which the authentication was performed, to the Aadhaar number holder or parent or guardian, in case of a child, at the time of authentication; and</p> <p>(d) record of consent of the Aadhaar number holder, or parent or guardian, in case of a child, for authentication, but shall not, in any event, retain the PID information.</p>	<p>Comments for Clause 18(1)(a) - For implementing of fraud checks during transaction processing, settlement & dispute in AePS financial transactions, UID, VID, UID token, & ANCS Token related information are used as identifiers. UIDAI may release additional clarification allowing for storing these details for the AePS transactions in a secure manner.</p> <p>As per said regulations the entities which are currently not using the authentication services have to maintained the logs for a period of 2 yrs in active environment and archived for a period of 5 years upon expiry. Suggest to revisit this clause.</p> <p>Clause 18 (1) (a) - Need to be relooked and logs may have UID token and TXN only. putting Aadhaar will put too load on Vault infrastructure and hence application performance and feel. Format of logs? What about HSM?</p> <p>Given the various provisions governing storage of Aadhaar number/ VID, we request the UIDAI to clarify both the instances in which a requesting entity is either permitted to store Aadhaar number or prohibited from doing so to avoid any ambiguities in the future.</p> <p>The requesting entity should expose a common way for the aadhaar holder to access purpose and content data. This data should be exposed in a single format across entities as defined by the authority.</p>
50	Retention and Disclosure of identity information and e-KYC data		<p>Currently, the Draft Regulations do not envisage a scenario where an entity can disclose the identity information or e-KYC data for legal or regulatory reasons or to authorities. We request the UIDAI to incorporate the below provision as an additional clause to the Draft Regulations, to deal with the scenario contemplate in the corresponding column here:</p> <p>"Notwithstanding anything contained in these Regulations, a requesting entity or Sub-AUA or Sub-KUA is permitted to disclose or share (including with any regulator or government agency pursuant to an order or directive) identity information, e-KYC data or Aadhaar data for compliance with requirement under applicable law."</p>

51	18 (2)	The logs of authentication transactions shall be maintained by the requesting entity for a period of 2 (two) years, during which period an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.	<p>Proposed revisions are provided in red: “The logs of authentication transactions shall be maintained by the requesting entity for a period of 2 (two) years, during which period an Aadhaar number holder shall have the right to access such information maintained by the requesting entity in the logs, in accordance with the procedure as may be specified.”</p> <p>Suggest to incorporate the definition of Logs and also in which format should logs be maintained?</p> <p>UIDAI is asking for logs of two years and 5 years while for UIDAI it is six months? same for ASA also ?</p> <p>We request the UIDAI to incorporate the below provision: "Notwithstanding anything contained in these Regulations, a requesting entity or Sub-AUA or Sub-KUA is permitted to disclose or share (including with any regulator or government agency pursuant to an order or directive) identity information, e-KYC data or Aadhaar data for compliance with requirement under applicable law.”</p> <p>A common procedure shall be created to access this data so that the account holder can access this easily.</p>
52	18 (3)	(3) Upon expiry of the period specified in sub-regulation (2), the logs shall be archived for a period of five years or the number of years as required by the laws or regulations governing the entity, whichever is later, and upon expiry of the said period, the logs shall be deleted.	<p>We would humbly request that this period for storage shall be reviewed based on past experience. In recent past we have not encountered any scenario where someone had to look at logs beyond few months.</p> <p>Logs storage for 7 years and 6 months is ambiguous and creates huge strain on the IT ecosystem - based on rough estimates considering 50 KB's of logs with current TSP volumes, it would need approx.. 1,192 GB / month which translates to approx.. 14305 GB / year</p>
53	19 (c)	On receiving the response from CIDR, transmit the result of the transaction to the requesting entity that has placed the request	<p>As mentioned in point no 2&3, additional clarification may be provided by UIDAI as a separate circular defining the requesting entity for AePS transactions:</p> <ul style="list-style-type: none"> - Acquirer bank, with respect to the point of transaction initiation and device registration - Issuer Bank with respect to billing and UID token response
54	19 (e)	Communicate to the Authority, all relevant information pertaining to any agreement that (ASA) may enter into with a requesting entity’	UIDAI to clarify whether any additional information, other than the current process of Engagement letter is required to comply with this clause.

55	19 (k)	Any value added service that an ASA provides to a requesting entity under a contract shall not form part of the Aadhaar authentication process.	UIDAI to clarify whether AePS banking services is considered as VAS. If yes then separate clarification/clause may be required to keep AePS services outside of this clause.
56	20 (1)	<p>20 (1) An Authentication Service Agency shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:-</p> <p>(a) identity of the requesting entity (b) parameters of authentication request submitted; and (c) parameters received as authentication response:</p> <p>Provided that Aadhaar number, Virtual Id, UID Token, ANCS Token, PID information, device identity related data and e-KYC response data, where applicable shall not be retained.</p>	<p>For implementing fraud checks, settlement & dispute on AePS based financial transactions, UID, VID, UID token, ANCS Token and Device Identity related information shall be required.</p> <p>UIDAI may release additional clarification allowing for storing these details for the AePS transactions in a secure manner.</p>
57	20A (1)(b)	any other data shared by the resident during the course of verification including mobile number, email id, photo etc;	<p>While we understand and accept the position for maintaining such data, we request UIDAI to clarify that this is limited only to offline verification process, to remove any ambiguity.</p> <p>We have proposed some revisions to the clause in view of the comments, where the revisions are provided in red: “any other data shared by the resident during the course of the offline verification including mobile number, email id, photo etc.”</p> <p>We understand this provision relates to the offline verification process, and have proposed a minor edit to clarify: “any other data shared by the resident during the course of the offline verification including mobile number, email id, photo etc.”</p>
58	20A (1)	“but shall not, in any event, store the Aadhaar number or Virtual ID of the Aadhaar number holder.”	We understand that such proposed by the Authority will be applicable prospectively.

	20A(2) Optional Maintenance of Logs by Offline Verification Seeking Entity	The OVSE shall not share the logs with any person other than the concerned Aadhaar number holder or for grievance redressal and resolution of disputes in accordance with the provisions of the Act. The verification logs shall not be used for any purposes other than those stated in this sub-regulation.	This should be replicated for requesting entity as well as it's a generic clause and customer can request for logs for any reason whatsoever. This is has to be read with Obligations of Requesting Entity.
59	21 (1) Audit of requesting entities, Authentication Service Agencies and Offline Verification Seeking Entities.—	The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including their Sub-AUAs and Sub-KUAs, Authentication Service Agencies and Offline Verification Seeking Entities, either by itself or through audit agencies appointed by it, to ensure that such entities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued by the Authority.	UIDAI to define the scope / threshold for conducting such audits. Qualification for audit for AUA/KUA & OVSE should be defined. 1. As per said para even if RE is not using authentication services the audit is mandatory. The said requirement should be waived off for those entities which are not using the said services. 2. Commuation/intimation/notice of minimum of 24 hours to be given to ASA and requesting entities before conducting audit of the ASA and requesting entity. We request the UIDAI that the clause should also bring in the purview of audit, the personnel of the requesting entity along their sub-AUAs and sub-KUAs which may be directly or indirectly involved in the operations of the authentication perusing Aadhaar data. Authority may ask for a periodic audit report generated by the ASA about operations, infrastructure, systems and procedures of requesting entities, including their Sub-AUAs and Sub-KUAs, Authentication Service Agencies. This report can be in a single format application for every ASA.

60	25 (1)	<p>the Authority may, without prejudice to any other action which may be taken under the Act, take such steps to impose disincentives on the requesting entity or an ASA for contravention of the provisions of the Act, rules and regulations thereunder, including suspension of activities of such entity or agency, or other steps as may be more specifically provided for in the agreement entered into by such entities with the Authority:</p> <p>Provided that the entity or agency shall be given the opportunity of being heard before the termination of appointment and discontinuance of its operations relating to Aadhaar authentication.</p>	<p>Timeline should be provided within which order of imposing disincentives by the Authority shall be heard before the final decision is to be taken.</p> <p>Also to mention if the requesting entity has right to appeal against revision order or not. This will help in the time management for the grievance of the entities and will help them to rectify their mistakes.</p> <p>We request the UIDAI to also decide and define the quantum of financial penalties commensurate with the default in case of a default by a requesting entity.</p> <p>Sub-section (1) may be added with an additional proviso at the end to state: “Provided further that where such failure independently amounts to be an offence under other laws, applicable for the time being, shall be additionally proceeded as per the concerned law.”</p>
----	--------	---	--

61	25(1A)	<p><u>Section 25 (1A)</u> Where any Offline Verification seeking entity,(a)fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time; is in breach of its obligations under the Act and these regulations;(b)uses the Aadhaar Offline Verification facilities for purposes other than those specified;(c)fails to furnish any information required by the Authority for the purpose of these regulations; or(d)fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority, the Authority may, without prejudice to any other action which may be taken under the Act, including such criminal action as it may deem fit, take such steps to impose disincentives on the Offline Verification seeking entity for contravention of the provisions of the Act, rules and regulations thereunder. Provided that the entity or agency shall be given the opportunity of being heard before any action is taken. (2)Any such action referred to in sub-regulation (1) may also be taken against any entity or Sub-</p>	<p>Sub-section (1A) may also be added with an additional proviso at the end to state: “Provided further that where such failure independently amounts to be an offence under other laws, applicable for the time being, shall be additionally proceeded as per the concerned law.”</p>
----	--------	---	--

62	27 (2) Duration of storage. —	Upon expiry of the period of six months specified in sub-regulation (1), the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by the order of a court not inferior to that of a Judge of a High Court or in connection with any pending dispute.	<p>This should be any court, some of the cases take time to reach High court or a Judge of a High Court.</p> <p>We request more detailed processes to be specified in respect to Aadhaar withdrawal request received.</p> <p>KYC is required to be maintained for 10 years beyond the termination of contract, In a scenario where the Aadhaar is withdrawn during the tenure of the policy, compliance expectations /maintenance of records for audits/ dispute, processes to be adopted, more clarity solicited.</p> <p>We request the UIDAI to increase the duration of storage of the data to 12 months to support verification enquiring / litigation evidences / investigations by the financial authorities etc.</p> <p>This provision seems contradicting to #20 above which mentions log storage duration as 2 years.</p> <p>Sub-section 2 may be replaced with the following: “(2)Upon expiry of the period of six months specified in sub-regulation (1), the authentication transaction data shall be deleted unless otherwise prescribed by a court order or a law applicable for the time being in force.”</p> <p>Limiting retention power orders only with High court will make it impractical since not in every case a high court may be approached. Since every court’s order comes with ‘judicial application of mind’, non-extension of this power to courts which are otherwise competent fails to prove any legal object. Such reservation of power with high court also leads to limits of rights of citizens to access justice.</p> <p>Additionally other than courts, other lawful authorities must also have power to order for retention of this data, as it may be important in law enforcement related duties of State [example – money laundering related cases under investigation or trial, etc.]</p> <ul style="list-style-type: none"> • The amendment to regulation 26 brings the Regulations in line with Puttaswamy II, where the SC had recommended this amendment to restrict the scope of metadata stored by UIDAI. • The amendment to regulation 27 will allow UIDAI to use authentication transaction data for business intelligence purposes. • However, the language is potentially misleading and a redrafted version is in the column 4.
----	----------------------------------	---	--

<p>63</p>	<p>28 (1) (2) (3) (4) (a)</p>	<p>(1) An Aadhaar number holder shall have the right to access his authentication records subject to conditions laid down and payment of such fees as prescribed by the Authority by making requests to the Authority within the period of retention of such records before they are archived.</p> <p>(2) The Authority may provide mechanisms such as online portal or mobile application or designated contact centers for Aadhaar number holders to obtain their digitally signed authentication records within the period of retention of such records before they are archived as specified in these regulations.</p> <p>(3) The Authority may provide digitally signed e-KYC data to the Aadhaar number holder through biometric or OTP authentication, subject to payment of such fees and processes as specified by the Authority,</p> <p>(4) The authentication records and e-KYC data shall not be shared with any person or entity: (a) other than with the Aadhaar number holder to whom the records or e-KYC data relate .. in accordance with the verification procedure specified. Aadhaar number holder may share their digitally signed authentication records and e-</p>	<p>What all we have to share...request for clarity for better understanding.</p> <p>We would like to seek clarification from UIDAI on the authentication records i.e. which all transactions would qualify under this parameter. Is there any prescribed format / mechanism that the entities should follow while sharing this information.</p>
------------------	-----------------------------------	--	---

64	28 (4) (b)	<p>Section 28. Access by Aadhaar number holder.</p> <p>—</p> <p>(4)The authentication records and e-KYC data shall not be shared with any person or entity:</p> <p>(a)other than with the Aadhaar number holder to whom the records or e-KYC data relate in accordance with the verification procedure specified. Aadhaar number holder may share their digitally signed authentication records and e-KYC data with other entities which shall not further share with any other agencies without obtaining consent of the Aadhaar holder every time before such sharing.</p> <p>(b)Except in accordance with the provisions of the Act.</p>	<p>There appears to be a typographical error in this provision.</p> <p>We request the UIDAI rectify this as follows:</p> <p>“(b)Except in accordance with the provisions of the Act and the regulations.”</p> <p>Such data may sometimes be required by lawful authorities. The same shall be provided and if necessary with prescribed procedural rules mandated for such acquisition [so that privacy concerns are taken care of too]</p>
65	Schedule A	<p>Schedule A- Eligibility criteria for appointment as requesting entities</p> <p>2. Technical and Financial criteria for entities for appointment as requesting entity are as under:.....</p> <p>Technical requirements.....</p> <p>[BOTH CATEGORY 2 & 3, POINT 4]:</p> <p>4. Organisation should have adopted data security requirements as per the IT Act 2000.</p>	<p>We recommend the inclusion of 'Payment System Operators' here to even cover future categories of licensed / authorised entities, such as Payment Aggregators.</p> <p>We recommend the inclusion of 'Payment System Operators' in Schedule A to cover future categories of RBI licensed/ authorised entities, such as Payment Aggregators.</p> <p>Point 4 – may be replaced with – “Organization should have adopted data security requirements as per the IT Act 2000 or other applicable Data Protection laws”.</p>
66	29 (2)	<p>Repeal of the 2016 Regulations</p> <p>29. Repeal and savings. –</p> <p>...</p> <p>(2) Notwithstanding the repeal of the Aadhaar (Authentication) Regulations, 2016, anything done or any action taken under the said Regulations shall be deemed to have been done or taken under the corresponding provisions of these Regulations.</p>	<ul style="list-style-type: none"> • This requires some changes to be legally valid. • Redrafted provision is in the column 4.

Other Comments

1	Since offline verification is fairly different from authentication in terms of its processes, conditions, safeguards etc., it is proposed that a new Chapter V be inserted
2	To make Chapter V, two types of changes have been made to the draft prepared by UIDAI:
3	The following clauses which deal exclusively with OV have been deleted from their original position and moved to the new Chapter V: Regulations 3A, 14A, 16A, 20A, and 25(1A).
4	The following clauses which relate partly to OV and partly to authentication have been split, and the latter portions placed in the new Chapter V with suitable modifications: Regulations 5, 6, 10, 21, and 22.
5	<ul style="list-style-type: none"> • There are two forms of authentication that UIDAI can consider adding (or at least creating the legal backing for through this amendment)- <ul style="list-style-type: none"> o Push notification on the mAadhaar app. With increasing smart phone penetration, this could become a highly-used method. Secure, decentralised tech is already available in the market, as shown by start-ups like Ensurity and Duo Security. o Token-based authentication, where Aadhaar holders can request for a 'token' (e.g. a chip-based card) at a fee. Estonia uses such a system for fully-decentralised authentication. UIDAI had decided against it initially due to cost - but can be made an optional service now & it is also possible that chip based card costs have come down since then. Has privacy advantages as well. • OTP can be sent through a voice-based method as well (e.g. person gets a call and a voice-based system reads out the OTP). Banks are using such tech. Will be better for less-literate populations. • Aadhaar regulations have had the “no denial of service” clause for years, yet we see it happen - e.g. to 1.5% of PDS users. Offline authentication may face similar issues. Therefore, we are sharing some ideas that will help, though you'd be the best judge on feasibility: <ul style="list-style-type: none"> o An explicit provision that those who are denied service due to auth failure (or non-profits representing them) can approach UIDAI for resolution. This would eventually help collate data to highlight areas of recurring failure which could be redressed along with relevant authorities. o This of course, if appropriate, could also be structured as access to the Aadhar ecosystem being dependant on offline verification being provided in cases where online verification fails (subject to UIDAI determination) • These regulations have several rights for Aadhaar users that they may be unaware of. Can UIDAI create and publicise a "charter of Aadhaar user rights"? • To make things easier, authentication logs should be available to the user on the mAadhaar app, and they should also be able to withdraw consent to a KSA/ASA there.
6	<p>For Businesses-</p> <ul style="list-style-type: none"> • We've seen that frequent changes in UIDAI rules in the past have hampered business continuity. Therefore, can these rules add that any change in access to the Aadhaar ecosystem is preceded by an 8-week public consultation, unless it is an emergency. The IBBI adopted such a “public consultation mandate” for its own regulations.

7	<p>For the past 15 months, the entire country is going through an unprecedented situation and many lost jobs, lives, and many are struggling to survive.</p> <p>In order to obtain some of the benefits the Gov offers, it is mandatory to have our mobile numbers updated in all the places.</p> <p>Can you please include the mobile number update as well through your UIDAI portal with the following conditions?</p> <ol style="list-style-type: none"> 1. OTP sent to the old number 2. OTP sent to the new number 3. Put a condition that the new mobile number should be in the name of the Individual who is trying to update the Aadhaar 4. Once the new mobile number is linked to Aadhaar, designate a phone number the user has to call to verify the mobile number 5. Send the OTP to the registered email ID to complete the process 6. Add an additional fee (may be upto Rs.500/-) to update the mobile number through online
8	<ol style="list-style-type: none"> 1.Call Centre Executive Shall Tell Every Information Like Pincode,Date Of Birth In Case Of Aadhar Operator Mistype Any Information Of Aadhar Card Holder . 2.To Know Aadhar Number Please Replace Pincode Verification By Giving Date & Time Of Enrolment Number. 3.N Case Of Resident Lost Aadhar Card And Slip Resident Can Download Their Aadhar Card Through Resident's Finger On Uidai Website. 4.And Upload Every Enrolment Slip On Uidai Website So Resident Can Download His/Her Enrolment Slip. <p>Because Lots Of People Still Does Not Get Their Aadhar Card.</p>
9	<p>My Suggestion for aadhar draft 2021 is before black listing aadhaar operators please listen to them also, and if complaining resident found guilty punishment and penalty also on resident</p>
10	<p>Aadhaar should provide exception case update after limit cross as many people are suffering to get DOB update . Please update DoB as per documents we have by verifying them .</p> <ul style="list-style-type: none"> •Marksheet can easily be verified online . •Passport can be verified.
11	<p>I have been trying to get my phone number on Aadhar changed for a long time! I went to the centre, but my biometric did not match. This should have been communicated at the centre itself. I had to wait 50 days to find this out. Now in the pandemic I have to do it again!! Even the online checking process is tedious, why should one write their reference number, and time and date. It should just be the reference number.</p>
12	<p>Linking mobile number with aadhar card should be done online</p> <ol style="list-style-type: none"> 2. Now to link the number, one has to go to the Aadhaar center where there are long lines and customers are upset. 3. At some centers, people go to get the mobile number updated and they are charged more by updating their complete biometrics. 4. So this facility should be opened to all. 5. In this, the facility of mobile number update should be enabled by logging in using biometric to identify the Aadhar card.

13	<p>Email address should be added/updated in UIDAI database, only after email verification. Like we do for mobile update.</p> <p>Currently I am receiving all authentication details of 4 people who are having First and last name same as me. I have reported this multiple times to help@uadai but there is no response.</p>
14	<p>Please Extend Date of Birth Revision Limit I have Passport Birth Certificate School College Certificate. Due to this premise, our life is being ruined, what should we do, since when there is no understanding behind you. I don't know about your new rule, my suggestion please check all documents than verify I am upset since one year bcz no job no claim any policy</p> <p>All document attach</p>
15	<p>1. After the death of a person, as of now we dont have a mechanism to unlink or disable his/her aadhaar/PAN and this easily allows people to do corruption. For example if a senior citizen father dies, son can still manage online transactions and other things (wherever personal intervention is not required) for at least 1 year or even more.</p> <p>Solution proposed:</p> <p>One solution is to link the death certificate with aadhaar, but it might be challenging. Making aadhaar entry in the death certificate mandatory is one option but might take time. As a quick implementation, AADHAAR MOBILE APP and WEB APP should have a finger scan mechanism and have to validate at least in a year to make sure the person is alive. Aadhaar service centers can also give this facility to the public. Public should get an SMS after so and so time (say 1 year) saying aadhaar will go to dormant state if not authorized in a month. If not done, aadhaar goes to a dormant state. If it is dormant for say 5 years, we can delete it from public usage and keep it only on the central server. (If any time needed later, the central server will have the details, but the public can't access it). Obviously the authentication issue can be addressed with a grievance portal. To add to it, the re-authentication process should be initiated only after OTP verification. If anyone is trying to tamper it, after so and so time failure, person needs to visit aadhaar center or needs to validate through video KYC call etc. Person should keeps getting warning for each and every authentication failure (count down)</p> <p>2> Next point. As of now aadhaar takes even small names, I mean abbreviations. For example my complete name is Kiran Kidavukunnil Paduvilan. Passport and PAN have it in complete. But aadhaar gives the option to say it as 'Kiran K P' This is a security lapse if a person is not linking with PAN or passport. So it is better to force the full name mandatorily. Or if a new aadhaar is being made, there should be a PAN also made along with it (if the person is not having a PAN).</p>

16	<p>The present draft needs to be inclusive of Senior Citizens, People of determination, People with limited mobility, People with Disabilities-the provisions of the Aadhaar program on the criterion of services provided for such individuals for the purpose of enrolment, modification of details etc should be clearly articulated in the draft. It is my recommendation that apart from the general public there should be specific mentions/provisions earmarked for the following sections:</p> <ol style="list-style-type: none"> 1. Senior Citizens in the age group between 65-75 years of age : For this category an option to enrol/modify the details online should be present and if there is a modification in the biometrics required in those scenarios there should be an option either to: <ol style="list-style-type: none"> 2. (a)Walk-in to an UIDAI centre nearest to their residence to be able to present their biometrics without having to wait in a queue through Customer Service representatives being educated for such scenarios or alternatively a separate Senior Citizen Queue for such persons. <ol style="list-style-type: none"> (b)In the case the person is presently not mobile due to medical conditions for a walk-in to the UIDAI centre nearest to their residence then the concerned may request UIDAI for collection of Biometrics from their residence at a nominal charge of Rs.25/- per visit and upon submission of a doctor's certificate citing their medical condition. 3. Senior Citizens above the age of 75: For this category, an option to enrol/modify the details online should be present and if there is a modification in the biometrics details required-a provision should be there for booking appointment for collection of biometrics at the person's residence without any additional charge to the senior citizen. The appointment for visit for biometrics collection may be altered for a maximum of 3 times post which a nominal charge of Rs. 50 should be imposed. 4. People of Determination / Differently Abled People / Disabled People & People with Limited mobility: For this category, an option to enrol/modify the details online should be present (subject to relevant documentation being provided and a medical certificate from a doctor citing the medical condition) and if there is a modification in the biometrics details required-a provision should be there for booking appointment for collection of biometrics at the person's residence at a nominal charge of not more than Rs.50 per visit.
17	<p>I request to you provide facilities online to mobile no update/ change , if user have already old mobile number and they want to change they need to just enter otp from both mobile number. U can charge for this service but if anyone want to add mobile number they need to visit aadhar center otherwise update/change mobile number should be online.</p>
18	<p>(1) Kindly design the physical shape of Aadhaar card like PAN card for keeping conveniently and</p> <p>(2) also do print QR code or BAR code or ANY other bank type code or Chip type sticker for accessing one's info or data if one's physical identification or impression fails which always happens when there is urgency. This suggestion will also helpful for the agency to get the true data when almost all impressions recognition fail however the electronic device will definitely need to be upgraded.</p>

19	<p>1. Offline Mobile number update - Many citizen just wants to Update there mobile number but due to long queue at Aadhar Seva kendra they just postponed it.</p> <p>2. Address update - In Many States we move for job and stay there for number of years but the main thing is we even cannot update Aadhar card for major document.</p> <p>3. Online Mobile Update - In this pandemic time UIDAI should allow everyone to Update there mobile number through online mode. Yes offcourse take some proof that the number belongs to them but allow it. It's very difficult to Update Mobile number through offline mode and for that many people cannot use there Aadhar card of opening anything online like bank account/demant account/etc</p>
20	<p>1. Updation of registered mobile number should be online without biometrics.</p> <p>2. There should be an option to get OTP On registered Email ID.</p> <p>3. During lockdown many centres are not working. I request you to look into this as a lot of bank work is not possible without adhaar correction. They should be open during lockdown.</p>
21	<p>1. Dedupe for >9 connections overall & restriction of 2 Connections/Day - Currently with the UID token the checks are performed to ensure compliance, however, the Authority is asking us not to capture UID Token, this will impact the validation, since Aadhaar Number too will be masked & is a very important data point for identification of subscriber with >9 connections.</p> <p>2. OVSE- Offline Verification Seeking Entity – Kindly clarify that we as Vodafone Idea Limited registered as ASA and AUA with the Authority can be treated as OVSE or we will have to apply afresh to become an OVSE, in that case what will be the process for the same, if any.</p>
22	<p>1. New regulations allow withdraw of consent by Customer and Entities to delete such records of Aadhaar. Feedback : Such clause conflicts with record keeping requirements under PMLA and can remove the trails causing frauds and audit issues. Recommend the clause to be amended / deleted.</p> <p>2. Aadhaar Authentication & Verification logs can be accessed by a customer by requesting the entity (Such Clix, Banks, etc). Feedback : This should be done only for grievance redressal and a prescribed fee.</p> <p>3) Records to be maintained on the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by the order of a court not inferior to that of a Judge of a High Court or in connection with any pending dispute. Feedback : This should be any court, some of the cases take time to reach High court or a Judge of a High Court.</p>
23	<p>With the Publication of the regulations , the AUA/ Sub-AUA, KUA/ Sub-KUA so authorized under these regulation shall deemed to have satisfy the requirement under section 11 A of the PMLA Act, 2002</p>
24	<p>Can Aadhaar OTP authentication be initiated using feature phones or do UIDAI envisage the use of Feature Phones for Authentication Services?</p>

25	<ul style="list-style-type: none"> • During Biometric or Online Aadhaar Authentication process, user should be able to choose which information he wants to be shared with the service provider and which information he wants to withhold. • For example, if the user wants to share only his name and address with the service provider, he can checkmark name and address on the authentication portal and leave rest of the fields viz. DOB, Real ID number, Mobile Number and Email Address unchecked.
26	<p>SMS NOTIFICATIONS</p> <ul style="list-style-type: none"> • After each verification event, the user should get an SMS message on his registered mobile number, indicating that his Aadhaar Number has been used to authenticate him. • SMS should also mention whether the authentication was successful or not and the merchant/business establishment/government organization where the authentication was performed.
27	<p>WATERMARKING</p> <ul style="list-style-type: none"> • If any Organization or Service Provider stores Scanned Copies of Aadhaar or Photos of Aadhaar or Photocopies of Aadhaar, it should be made mandatory for that organization or service provider to apply a non-removable watermark on the Scanned Copies/Photos/Photocopies of Aadhaar Card. • Watermark should mention name of the organization, date, time and location of collection of Scanned Copy/Photo/Photocopy of Aadhaar Card. • Watermarking will prevent misuse of Scanned Copies/Photos/Photocopies of Aadhaar and help in identifying source of data leak in the event of data leak at organization/service provider. • For example, if ICICI Bank stores Scanned Copy of Aadhaar Card of a customer, it should apply a watermark of ICICI Bank on the scanned copy of Aadhaar Card along with date, time and location. If any data leak/ data theft happens at ICICI Bank, it can be determined from the watermark that the data leak happened at ICICI Bank and the leaked scanned copies of Aadhaar Card cannot be misused anywhere else because the name of ICICI Bank, date, time and location is already watermarked on the Scanned Copy of Aadhaar Card.
28	<p>RIGHT TO RECALL/ RIGHT TO BE FORGOTTEN</p> <ul style="list-style-type: none"> • No organization, service provider or person should be allowed to retain Aadhaar Data belonging to the user against that user's will. A user should have rights to instruct the organization or service provider to delete Aadhaar data belonging to him.
29	<ul style="list-style-type: none"> • The real ID number (Aadhaar Number) should not be printed on the ID card, only virtual ID number (Virtual Aadhaar Number) should be printed on the ID cards. • During authentication process, only financial organizations can ask for the real ID number (real Aadhaar Number) of the citizen. • Non-financial organizations should not be allowed to check the real Aadhaar number of the citizen. • Non-financial organizations should be provided with only demographic information. This will protect privacy and prevent profiling of citizens.

30	<ul style="list-style-type: none"> • Different types of identity access levels can be defined for different types of organizations. • LEVEL A - Financial organizations can be given level A access. In level A access, full ID details (real ID number, Name, Gender, DOB, Address) can be accessed by the financial organizations. • LEVEL B - Telecom organizations can be given level B access. In level B access, telecom companies can access virtual ID number, name, gender, DOB and address of the citizen. • LEVEL C - Retail and hospitality (hotels) can be given level C access. In level C access, the hotels can access only name and address of the citizen. • LEVEL D - Other requesting authorities and individuals can be given level D access. In level D access, the access should be limited to checking the validity/authenticity of the card/demographic information. • This differential access will ensure security without sacrificing privacy.
31	<ul style="list-style-type: none"> • Hotels, landlords, hosts and recruiters/employers don't need to collect and store ID documents of the customers/tenants/ employees/household helpers etc. They can perform level C authentication and keep the authentication token slip saved with them. • In case of any crime or fraud, the hotel/landlord/host/employer just need to show this authentication token slip with police. Police can then use authentication token number to fetch more details about the person from the central verification agency.
32	<ul style="list-style-type: none"> • To prevent concentration of all authentication data in one ID verification agency, an escrow agency can be sandwiched between the central authentication agency and the verification requesting authority, for level C authentications. • That means if a citizen, authenticates his identity at a bank, mutual fund house, insurance company, telecom company or at a gas agency, his authentication details will be stored by the central authentication agency. • But for level C authentications (online account verification, hotel stay, air travel, house rent, car hiring), the authentication logs will be maintained by the escrow agency. • Different escrow agencies can be setup for different types of authentication e.g. Online accounts, Hotel stay, Air Travel, Train Travel, House rent, Car hiring etc. • So, the authentication data will get dispersed across multiple escrow agencies. This will prevent concentration of data at one organization.

33	<ul style="list-style-type: none"> • ID cards should be secure and revocable just like Debit cards. • We should give identity the same importance as we give to money. • Just like there are banks for money, there should be IDENTITY BANKS for storing and authenticating identity and DATA BANKS/INTELLECTUAL PROPERTY BANKS for storing intellectual property of the citizens. • No one can steal your money, if he has stolen your debit card or has scanned copy, photo or photocopy of your Debit card or bank passbook. Similarly, no one should be able to steal your identity using your stolen ID card or using a scanned copy, photo or photocopy of your ID card. • Just like banks issue statement of your transactions, ID verification agencies (UIDAI) should issue ID verification/authentication passbook for each ID. • The same identity verification agency (UIDAI) can also be entrusted with authenticating educational certificates, property registration, automobile registration and business registration. • A NetIdentity interface (analogous to NetBanking) can be built, where citizens can check their authentication history. • For issuing identity cards (Aadhaar Cards), changing card PIN, resetting NetIdentity password, or making correction to ID details, existing infrastructure of Public Sector Banks can be utilized. • Identity should flow like money. When you perform an authentication, one token should be deducted from your identity account. Each user will get 1000 authentication tokens. When those tokens are utilized, his account will be replenished with another set of 1000 tokens. The purpose of this countable token system is to detect any unauthorized usage of identity.
34	<p>In addition to Biometric and OTP Authentication, you should add the following modes for Aadhaar Authentication -</p> <ul style="list-style-type: none"> (1) Chip/QR Code/VID + PIN (just like Debit Card) (2) Chip/QR Code/VID + Password
35	<ul style="list-style-type: none"> ● Multi-factor Authentication - Identity verification through just Photocopies, Scanned copies and Paper/Plastic ID cards is single factor authentication. Single factor authentication is inadequate and risky, as criminals can use stolen digital and physical identities. - Multi-factor authentication should be made mandatory, in which citizens will have to use 2 or more methods simultaneously to verify their identity. People who are concerned about security, can choose 3 or more factors. People who like convenience, can choose only 2 factors. - Chip + PIN + OTP - Chip + Password + OTP - Chip + PIN + Password + OTP - QR Code + PIN + OTP - QR Code + Password + OTP - QR Code + PIN + Password + OTP - Virtual ID Number + PIN + OTP (Online) - Virtual ID Number + Password + OTP (Online) - Virtual ID Number + PIN + Password + OTP (Online) - Virtual ID Number + PIN + Password + FIDO U2F key (Online)

36	<p>Aadhaar operators provide services to download and printout eAadhaar cards. eAadhaar cards of thousands of people remain stored in personal computers of such Aadhaar operators. These eAadhaar cards can be sold to unscrupulous elements or can be stolen by unscrupulous elements through malware and during laptop repair. If a criminal who has bought or stolen eAadhaar cards from Aadhaar operators, takes printout of these Aadhaar cards and use them to checkin hotels, book rail and air tickets, buy SIM cards, open Bank Accounts, authenticate fake accounts on Facebook and other online services; how will you prevent such misuse? Paper Aadhaar cards are very easy to fake (any good graphic designer can create fake Aadhaar Card) and eAadhaar Cards are very easy to get stolen by criminals from laptops of Aadhaar operators. Paper Aadhaar Cards and eAadhaar Cards are being accepted everywhere without any Biometric Authentication.</p>
37	<p>Attempt to broaden the limitations placed by the Puttaswamy judgement on Aadhaar The Puttaswamy judgement on the validity of the Aadhaar Act laid out certain red lines on which entities can lawfully use Aadhaar. The majority judgement struck down Section 57 of the Aadhaar Act, 2016 which enabled private entities to access Aadhaar related data. The 2019 Amendment permitted a variety of private entities to verify the identity of their clients by authentication or offline verification of Aadhaar. The Amendment did contain an important safeguard by specifying that individuals must be given the choice to not use Aadhaar to verify their identities; but there was little enforcement of this. The draft regulations specify that any private entity fulfilling the criteria, which includes regulated financial sector entities, telecommunications companies, and any corporation, are eligible to be authentication entities. We are concerned that the Regulations give the UIDAI wide leeway in which entities are allowed to demand Aadhaar, and do not impose any penalties or other obligations on entities that do not offer meaningful alternatives to Aadhaar-based verification.</p>
38	<p>The offline verification modes reduce security</p> <p>The Aadhaar project was originally designed for two modes of verification: checking the biometric or demographic details with the corresponding data saved in the CIDR (Central Identities Data Repository), or through a “one time password” sent to the mobile number linked to the Aadhaar number. However, as this mode of verification required an internet connection, a phone connection, and for the details to match, the technological and practical barriers caused exclusions, preventing residents from being able to access public services they were entitled to and suffering harm. In practice, many entities were merely referring to the Aadhaar “card” - the print out of the document generated by the Aadhaar ID - as proof of identification; much as they would refer to other photo IDs. However, the Aadhaar card, while being mandated in several places, has no basis in law.</p> <p>The 2019 Amendment Act introduced several different methods of offline verification, presumably in an attempt to paper over this gap between the reality of Aadhaar mandates and the law. The Regulations bring further clarity to these modes of offline authentication-</p> <p>Under Rule 3A, the formalization of the process of offline verification is an acknowledgment of the difficulties that online authentication posed to the target population. However, this risks moving towards a free for all wherein duplicate Aadhaar letters may be produced and Aadhaar authentication may be done on the basis of authentication factors not envisaged under the Aadhaar ecosystem.</p> <p>Such practices have already existed in many sectors wherein signed copies of Aadhaar cards were accepted as authenticated identity proof. It seems that this provision is intended to “grandfather-in” existing not approved banking sector practices of authorizing the use of paper copies of the Aadhaar proof of registration letter. It should be noted that this regulation mentions, for the first time in a legal document, the term “aadhaar letter.”</p> <p>Providing alternative methods of authentication for users is an important step, and could help make Aadhaar more inclusive. However, doing this without an acknowledgment of how checks will be enforced would cause difficulties. The UIDAI takes no responsibility for the sanctity of offline verification; or on how they are planning to enforce the guidelines set to AUAs.</p>

39	<p>Formalisation of the Virtual Identity Number</p> <p>Under rule 4A, the Virtual Identity Number (VID) has been formalised into operation. This is a welcome, albeit late step to enable the masking of Aadhaar numbers from databases of various entities which use Aadhaar based authentication. There have been multiple cases in the past where Aadhaar number based databases have been created by private organisations as well as government entities. These databases have seen data leaks and have been linked with other similar databases, compromising the privacy of users. Multiple VIDs for each Aadhaar number for authentication purposes would help inhibit the creation of such databases and thus be one step towards providing increased privacy to users.</p> <p>We further recommend that more awareness be created among people in India regarding VID to increase adoption of VID and steps be taken to ease the provision of VIDs to people in India. Further, more needs to be done to ensure that Aadhaar numbers are cleared from existing databases. It should be noted that in the Aadhaar judgement, the dissenting judgement recommended that the UIDAI ensure that Aadhaar data held by private entities was deleted. However this does not seem to have been done even till date - and should have been the subject of rule-making and executive action to enforce the Supreme Court’s direction.</p>
40	<p>Purpose limitation and “Presumed consent”</p> <p>Rule 17(iii)(d) introduces the notion of purpose limitation for Aadhaar-related data which AUA's access. However, this contains a problematic clause where consent for using data beyond the previously consented purpose is "presumed," if upon receiving information of how their information will be used, a user provides no response. This is a concerning provision and does not meet the established standard of purpose limitation. A change in the contours of consent must require fresh consent to be obtained by the AUA rather than just a notification requirement, as prescribed under the Regulation. Particularly in the context of a country where many people are unlettered; this is an example of "consent washing" and would dilute the principle of purpose limitation, which we have flagged in the past.</p>
41	<p>Facial authentication within the definition of biometric authentication</p> <p>Under the definition of biometric authentication (Rule 2), the inclusion of “other biometric modalities” opens up the possibility of the use of facial authentication and other biometrics means of authentication. While the Aadhaar Act, 2016 provides similar ambiguity regarding the definition of biometrics, it is essential that regulations provide more specificity. Facial authentication raises serious implications for users, over and above perhaps other biometric based authentication. As compared to other biometrics, facial data can be easily captured in a pervasive manner - and even without the know and consent of the user. The use of facial authentication opens a pandora’s box, and requires wide, inclusive and deliberate discussion. Until such discussion and engagement, facial authentication must not be considered for Aadhaar, and any plans must be put on hold at minimum.</p>
42	<p>Deletion of data on consent withdrawal Under Rule 6, a user has been provided greater rights over their data, wherein they are provided a right to withdraw their consent after authentication and an obligation is placed on the requesting entity to delete such user’s data. This is a helpful provision as it provides users greater autonomy on their data and also prevents the creation of databases full of inactive users with their personal data present. However, this is only applicable to data which AUAs have access to.</p> <p>We request that steps be taken to ensure that these rights are communicated to the user in a better manner, and the UIDAI come up with rules which make offboarding for users and subsequent deletion of data as easy for users as onboarding and sharing data</p>

43	<p>Notification on authentication of Aadhaar</p> <p>Another positive step in the Regulations pertains to the obligation on requesting entities to notify the user when any authentication request is placed for their Aadhaar number. This is a positive step which provides users greater transparency over the use of their Aadhaar and access to their sensitive personal data in the CIDR for the purposes of authentication by requesting entities. However, requesting entities must be required to ensure that they do not maintain a log of such notifications beyond a very limited time period - in order to prevent these user-empowering notifications from being used to construct a data trail that instead imperils privacy and enables surveillance.</p>
44	<p>Provision for Aadhaar Locking</p> <p>The Rules provide the legal recognition of the provision of Aadhaar locking, wherein apart from biometrics, any authentication based on the Aadhaar number of an individual can be locked by the Aadhaar number holder. This allows users greater control over their Aadhaar number and personal information associated with this number by giving them the option to disallow further authentication requests.</p> <p>However, there still does not seem to be an option for a user to delete an Aadhaar account altogether and get their data deleted from the CIDR. Since Aadhaar is a voluntary service, users must be given the right to get off the platform after enrollment.</p>
45	<p>Data retention by Requesting Entities</p> <p>Rule 18 of the draft regulations mandates requesting entities to retain logs for 2 years, and archive these logs for another 5 years. This is an excessive period of time. Transaction logs contain important metadata about the user, including the services they use, their location etc.</p> <p>Permitting the requesting entities to enforce this would be detrimental to the privacy rights of users. Recognising the sensitivity of metadata, the Supreme Court, in the Puttaswamy-II judgement on Aadhaar, ordered the UIDAI to ensure that Aadhaar authentication logs are deleted after 6 months. This appears to be violated by the current text of this Rule.</p>