THE REPORT OF THE TECHNICAL COMMITTEE ON INFORMATION UTILITIES

Part 1

Dr M. S. Sahoo,
Chairperson
Insolvency and Bankruptcy Board of India
7th Floor, Mayur Bhawan
New Delhi 110001

Date: 16th August, 2017

<u>Sub: Technical Standards under IU Regulation 13</u>

Dear Sir,

As per terms of reference we had deliberations in the Technical Committee on the drafting of Technical Standards for Information Utilities under Regulation 13.

Please find attached a consolidated report on 14 topics of the Technical Standards out of the 18 listed under the Regulation 13(2). Report on the remaining four topics will be submitted separately in the near future.

Regards

Dr. R. B. Barman,
Chairperson,
Technical Committee of IBBI

(Dr. Nand Lal Sarda)   (Dr. Pulak Ghosh)   (V.G. Kannan)
    Member   Member   Member

CONTENTS

A.   Acknowledgements

As Chairman of the Technical Committee on Information Utilities, I have had the privilege of recommending to lay down the Technical Standards ensuring and enforcing the reliability, confidentiality and security of financial data to be stored by information utilities. Information utilities (IUs) are a novel concept with no exact equivalents in the whole world. Therefore, while laying down the Technical Standards for this new kind of entities, which shall provide high-quality authenticated information about debts and defaults for resolving matters of insolvency and bankruptcy in a time-bound manner, it was important to have a clear idea of the services that are already being provided by other existing registries handling financial information and the commonality between their contents and processes with those required for rendering core services by IUs. The Committee is thankful to Dr. M.S. Sahoo, Chairperson, Insolvency and Bankruptcy Board of India (IBBI) for briefing us on the role of the Technical Committee under the regulations and explaining the background of underlying law along with the expectations from the Committee. Dr. Sahoo also guided the Committee at different stages to keep us focused on various issues. IBBI also arranged for presentations from TransUnion CIBIL Ltd., CRILC of RBI, CERSAI and MCA21. The Committee is thankful to Ms. Harshala Chandorkar, COO, CIBIL, Mr. R. Ravi Kumar, CGM, RBI, Mr. Shashi Raj Dara, Deputy Director, MCA and Mr. Praveen Kumar Sharma, MD & CEO, CERSAI for taking us through the processes and products of their respective registries. The presentations helped us to understand the information in their custody, the technology they use, processing and flow of information by them, and the possibility of leveraging the information available with them by IUs and vice versa.

The Committee then embarked on its mandate to lay down the Technical Standards. Mr. Shiva S. Ramann, MD & CEO, NeSL, (Company which has in-principle approval to establish IU) has provided excellent support to the Committee. He arranged the demo of submission and receipt of information and access to such information by users along with authentication of a digital agreement by using e-sign modality, in giving an understanding of storage of physical records by trustee companies for which we thank Mr. Amit Joshi, ECS Limited and Mr. Vinoth, ECS Limited. Mr. Ramann made a presentation on the process of Registration of Users and Unique Identifier for Registered Users also and provided valuable inputs based on his discussions with the user group of banks formed with the help of IBA.

The Committee is thankful to Dr.(Ms.) Mukulita Vijaywargiya, Whole Time Member, IBBI for making a presentation on the process that a Bank follows that makes its records sacrosanct under the Bankers' Book Evidence Act, 1891 and summarising the case laws relating to authentication and verification expected by an IU.

The presentation on Blockchain technology by TCS team comprising of Mr. Pradeep Gupta, Senior Client Partner, Nilesh Khedikar, Lead Solution Architect, Raghunath Ganta, Expert-Banking Technology Group, R Sundararaman, Lead SME for TCS BaNCS Banking Solutions, Anand Athani, Lead Architect for TCS BaNCS Banking Solutions representatives provided the

Committee updates not only on the newest developments in this field, but the pros and cons of Blockchain technology vis a vis the conventional technology for use by IUs. We are also thankful to Mr. Anilkishen Dukkipatty, Elemental Labs Pvt. Ltd. and his team for apprising the Committee on using Blockchain technology in developing PoC for NSE for a central KYC application across the banks having similarities with the functions of IU.

The Committee is thankful for discussions and contributions by Dr. Navrang Saini, Dr. (Ms.) Mukulita Vijayawargiya and Ms. Suman Saxena, Whole Time Members of IBBI. The team at the NeSL, specially Mr. S. Raghunatahan, Exec. Director, NeSL and Mr. Debasis Pal, Vice President, NESL, identified possible use-cases and made available comprehensive inputs to the Committee under the guidance of Mr. Rajesh Doshi for detailed deliberations. They did a wonderful job to deliver the detailed report also within the hard limitations on time.

Without the immense efforts of all those named above, the Committee could not have accomplished the tasks at the required level of quality. All the members of the committee join me to express our gratitude to all for the enormous contributions from each one to accomplish the task at hand.

Dr. R. B. Barman

B.   Abbreviations

API	Application Programming Interface
BCP	Business Continue Plan
CERSAI	Central Registry of Securitisation Asset Reconstruction and Security Interest of India
CIBIL	Credit Information Bureau (India) Limited
CIN	Company Identification Number
CRILC	Central Repository of Information on Large Credits
DR Facilities	Disaster Recovery Facilities
DSC	Digital Signature Certificate
IRP	Insolvency Resolution Professional
IBBI	Insolvency and Bankruptcy Board of India
IT Act	The Information Technology Act, 2008
IU	Information Utility
LLPIN	LLP Identification Number
MCA	Ministry of Corporate Affairs
NeSL	National E-Governance Services Limited
OC	Operation Creditors
OTP	One-Time Password
ROC	Registrar of Companies
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOAP	Simple Object Access Protocol
UDI	Unique Debt Identifier Number
UIN	Unique Identification Number
UIDAI	Unique Identification Authority of India

C.   Scope and Assumptions

The document consolidates the technical standards proposed for various topics listed in Regulation 13 under Chapter IV of the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017 (IU Regulations). The matters covered in this report are by way of the following Sections:

Section I	Registration of users (Regulation13(2)(c))
Section I	Identification and Verification of Persons (13(2)(f))
Section II	Unique identifier for each record and each user (13(2)(d))
Section III	Submission of information (13(2)(e))
Section IV	Authentication of information (13(2)(g))
Section IV	Verification of information (13(2)(h))
Section V	Standard terms of service (13(2)(b))
Section VI	Consent framework for providing access to information to third parties (13(2)(j))
Section VII	Data integrity (13(2)(i))
Section VII	Security of system (13(2)(k))
Section VII	Security of information (13(2)(l))
Section VIII	Risk management framework (13(2)(m))
Section IX	Preservation of information (13(2)(q))
Section IX	Purging of information (13(2)(r))

Technical Standards related to remaining four topics under Regulation 13 will be notified separately.

While setting up the Technical Standards, the Technical Committee of IBBI has been conscious not to prescribe any specific choice of technology or platform, so that each IU can exercise its own choice. Instead the Committee recommends IUs adopt robust data governance standards to take care of complete integrity of the IU database. In order that a single version of truth can be established, there should be unfettered access to data among the IUs, while each IU is free to maintain its own repository of mutually exclusive and exhaustive data.

D. Section I — Registration, identification and verification of user

13(2)(c) - Registration of users

13(2)(f) - Identification and Verification of Persons

The standards for registration of users and for identification and verification of persons should cover the following key objectives:

1. The Registration of any User will be done by an IU before any service is provided.

2. Identity of User will be verified based on a single primary identifier type. The access control shall ensure that any user is uniquely identified by the primary identifier that is issued by a government authority. Multiple types of ID option should not be allowed for the same category of Users.

3. The extent of verification of the Identifier taken from the User by the IU, shall determine the quality of evidence that shall attach to the authentication process that is facilitated by the IU.

4. The Registered list of Users and their UINs shall be shared with others IUs.

5. The digital signatures are at the core of the IU processes and a directory of digital signature certificates shall be maintained by an IU as part of registered user data for future reference or validation.

6. An IU should monitor the registration and user administration activities.

Technical Standards 13(2)(c) and 13(2)(f)

1) Registration should cover the following

   a) Capture of minimum required information as specified in these guidelines covering identity and contact details

   b) Deduplication check across IUs to ensure same person is not already registered

   c) Verify identity of the person against original issuer of ID

   d) Upload of Digital Signature Certificate (if available) and verification of the same with certifying authorities

   e) Acceptance of terms of usage

   f) Payment of fees as applicable for the IU

   g) Allotment of Unique Identifier Number (UIN – described under Section II of the Report)

   h) Issuance of user ID and password

2) **Individual persons** will need to provide only their Aadhaar ID at the time of availing IU services.

   a) The Aadhaar based process will apply to all Indian residents and any other individual persons holding Aadhaar.

   b) IU will do a deduplication to check if the same Aadhaar number has already been used previously in the same IU or another IU.

      i) If a match is found, i.e. where the person has earlier verified his/her credentials, IU needs to only perform identity verification against UIDAI database. The process will require mobile based OTP confirmation or biometric verification of credentials.

      ii) If no match is found, IU should verify identity against UIDAI database and also fetch other related demographic particulars including date of birth, address, mobile number, email ID as per UIDAI records and use the same for internally creating a registration record automatically.

   c) No user ID/ password needs to be issued to individual person with Aadhaar.

   d) For non-resident Indians or foreign individuals, IU should provide alternative mechanism to accept other supporting documentation.

3) For a **legal entity,**

   a) IU should collect registration information covering the entity as well as an authorised representative undertaking the registration process. Following details are to be covered:

      i) Name of entity

      ii) Type of person/ Legal constitution (e.g. Company, LLP, Partnership, HUF, Society etc.)

      iii) Indian/ Overseas status

      iv) PAN as the primary ID

      v) CIN/ LLPIN (if registered with MCA)

      vi) Date of incorporation

      vii) Representative person's full name

      viii) Representative designation

      ix) Aadhaar ID for the representative

      x) Primary Email ID

      xi) Alternative Email ID

      xii) Primary Mobile number

      xiii) Alternative Mobile number

      xiv) Landline number (if available)

      xv) Registered office address with PIN

xvi)   Communication address with PIN

b) The IU needs to perform a **deduplication check** first within its own database and also against the shared list of registered users of other IUs (as provided under Regulations 18(6)(b)) to check if the legal entity is already registered. This will be on the basis of the PAN of the legal entity.

   i)   If a match is found, the user will be informed and asked to login.

   ii) If the deduplication returns no match, the IU should verify the PAN with the issuing authority (IT Department database)

   iii) For the representative of the legal entity being registered along with the entity, the Aadhaar ID should be checked with UIDAI through OTP/biometric process

c) As part of registration process, the person registering on behalf of a legal entity should submit the **digital signature certificate (DSC)** of the legal entity, at the earliest opportunity. Else the same must be submitted before digital signing of a submission or authentication can be performed.

   i)   For legal entity, IU should verify such DSC, when submitted, to check if it is a valid one

   ii) In addition, IU should check if the name of the legal entity as per the registration data matches the organisation name as per the DSC. The name of the representative person as per DSC should also be checked against the identity as per Aadhaar.

   iii) In case the name of organisation and the representative both matches in (ii) above, no further supporting documentation will be needed and registration can proceed.

   iv) Where DSC information does not match registration data or DSC is not submitted, the registering person will need to upload softcopy of supporting documentation from the organisation to IU in order to confirm that the registering person is authorised to represent the legal entity. In case of a Power of Attorney based authorisation, such authorization shall be checked against the resolution of the Board. In such situation, IU will need to check the content of the documentation and approve such registration request.

   v)   **Email ID and mobile number** provided during legal entity registration need to be verified by sending appropriate message with OTP/ verification link to the email ID and mobile number. IU system should use only verified contact information. No verification of postal address is required to be performed by the IU.

4) Before completion of registration, the registering person must accept the **terms of usage** as specified by the IU. This will also apply to individuals accessing through Aadhaar validation.

5) Registration process will be completed with PAN (legal entity) or Aadhaar (individual) being treated as the **Unique Identification Number (UIN)**. In case of non-resident Indians or foreign nationals, UIN will be issued by the IU.

6) The IU will send a **confirmation mail** on completion of registration. For a legal entity, IU will also issue a **Login ID and a Password** through the preferred contact mode of email ID or mobile number for legal entity user. When such person logs into the IU portal for the first time, he/she will need to provide a second factor as credential in the form of date of incorporation and will be forced to change the password on first use.

7) The representative of a legal entity can access all IU services on behalf of the legal entity by using Login ID and password issued. For legal entities, the first registered representative user will be allowed to **create additional users** by using the User Administration function in the IU portal. Creation and administration of other users will be the responsibility of and under the direct control of the legal entity's registered representative. IU will not verify identity of any additional users created under the authority of the registered authorised representative of the entity.

8) Where the legal entity (such as banks or other creditors) wants to implement server based automated process for digital signature and submission, specific type of digital signature certificate (DSC) meant for installation on server will also need to be registered under a person belonging to the legal entity.

9) IU should monitor the registration and user administration activities including those being performed at the end of the legal entities, in order to identify any unusual pattern such as accounts remaining dormant for a long period. This and other surveillance mechanism will be addressed under Section VII and VIII of the Report.

***

D. Section II   Unique Identifier

13(2)(d) Unique Identifier for each record and each User

The standards for unique identifier for record and each user should cover the following:

1. The allotment of Unique Identifier to a User will be done by an IU after completion of Registration Process. The process & technical standards that are followed for Registration process have been explained in Section I above.

2. For allotment of Unique User Identifier Number (UIN), the broad technical standards proposed are primarily based on the primary identifiers i.e. PAN or Aadhaar Number.

3. For allotment of Unique Debt Identifier Number (UDI), the broad technical standards proposed are based on the combination of Loan Account Number allotted by the Creditor plus UIN of the Creditor (e.g. PAN), thereby making it unique. The pattern is elaborately narrated in the next Section on "Detailed Technical Standards planned" for the purpose.

4. The IU shall create and maintain appropriate list of Registered Users, the Unique Identifiers of Registered Users and the Unique Identifiers assigned to the Debts.

5. The IU shall also make the lists created as above, available to all Information Utilities and the Board.

Technical Standards 13(2)(d)

Unique Identifier Number to Users (UIN)
1. Aadhaar Number for individual users and PAN number for all legal entities should be directly used as UIN. Depending on the type of person, the PAN or Aadhaar field will be used as the identifier.

2. The Unique Identifiers would be as under:
   - For Individual Users (Aadhaar Number) (12 Digits) : ex. **469485907737**
   - For Legal Entity : (PAN Number) (10 Digits): ex. **AADPU6217E**

3. A key benefit of using the ID itself as the UIN is that there is no need for the creditors (and for the users) to store any new number issued by IU in their respective systems.

All systems at the creditors' end will already have provisions for PAN and Aadhaar fields. Hence, implementation of IU interface will be easier. Further, even users do not need to remember any new number assigned to them.

4. For non-resident Indian individuals or foreign nationals/entities, not covered by Aadhaar or PAN, IU should assign a new number since no fixed document type is applicable. The UIN in such case should be a serial number issued by IU, starting with IU code (1 digit), single digit indicator for type of person, followed by a 10-digit serial number e.g.

   o For non-resident/foreign individuals: 110000000023 (1 for IU code, 1 for Individual and serial number 23)

   o For overseas entity: 120000000009 (1 for IU code, 2 for legal entity and serial number 9.

Unique Debt Identifier (UDI)

5. UDI is planned as combination of creditor's identity (UIN) combined with the loan account number allotted by the creditor. Prefixing of creditor identification (PAN or Aadhaar) is necessary for uniqueness of UDI since it is possible that two creditors may have issued the same loan number.

6. In most situation, the creditor will be a legal entity with PAN (10 digit) as the UIN. However, in some situation (e.g. P2P or Operational Credit) an individual can also be a creditor. In such situation Aadhaar ID (12 digit) will be UIN. To ensure that loan number can be easily derived from the UDI, in case PAN number is applicable as UIN, two digits of 00 will be inserted after PAN and before loan account number so that loan number always starts from 13th digit of UDI.

7. UDI (total digits 32 max) will look like:

   o If PAN is AADPU6217E and loan a/c no is 12345678900987654321, UDI will be **AADPU6217E0012345678900987654321**

   o In case of individual creditor with Aadhaar no 469485907737 and loan number of HP/01283/2017-18, the UDI will be **469485907737HP/01283/2017-18**

8. The key advantage of this approach is that the loan number as existing with the creditor is retained and no new number is introduced. Deduplication check for new loan record is also easier since the UDI list is shared across IUs and knowledge of just the UDI is sufficient to run deduplication.

9. However, there are some disadvantages.

- o Primary one being the non-standard structure and field size for loan numbers across creditors.

- o Second the overall UDI size is long (30 digits).

- o Third, it is quite possible for the loan numbers of a creditor to undergo changes due to change of loan system or merger of two entities and their systems. Creditor may start reporting with a new loan number from a certain time, while IU will need to keep UDI unchanged, hence need for a mapping of UDI with creditor's new loan number is unavoidable.

***

D. Section III   Submission of Information

13(2)(e) Submission of Information

The standards for submission should cover the following:

1. All submission of information must be done with digital signature of the submitter
2. All Form C data, except default reporting, for a debt should be submitted in one file. A single submission file may have data about multiple debts.
3. Updated data submission will be in the same format of Form C.
4. Supporting documents to a debt or security can be submitted for a debt separately at any time.
5. Default can be reported at any time by the creditor in Form C.
6. Submission of balance sheet/ cash-flow and also submissions by IRP will be done at debtor level.
7. Any error, if comes to the notice, can be marked erroneous by the submitting party only.
8. An acknowledgement is to be issued to the submitting party on receipt of any submission of data/ document.

Technical Standards 13(2)(e)

1) Any information submission, whether in data format or as a document, must be **digitally signed** by the submitter. Digital signature should be of requisite class as specified in the standards for security of information under Section VII of the Report. Individual submitter can opt for Aadhaar based e-sign.
2) Submission of debt related data should be made together in the **same file** i.e. submitter identity, related party information and security information should be part of the same file containing the debt information which also includes outstanding liabilities.
   a) The format for such submission will as per **Form C placed as annexure,** with minor revisions.
   b) The 'other party' section of Form C will be repeated multiple times in the same file depending on number of parties connected to the debt
   c) Similarly, security details will also be repeated as many times as there are securities linked to the same debt. Where a single security is linked to multiple debts, each record of debt should accompany the same security data as linked information.
   d) The section on default (Form C in Annexure) will not be part of the regular debt data submission but will be undertaken only at the time of reporting of default.
3) Submission of **supporting documents**: Documents can be submitted at any time, not necessarily along with Form C data submission. Such documents should support multiple formats including PDF and scanned image files. All document submissions must also be digitally signed by the submitter.

a) Each supporting document for debt should have debt unique identifier reference

b) Each supporting document for security should have security identifier reference, which will be the CERSAI ID.

4) **Default reporting**: creditor may report default of a debt with reference to a specific debt. For reporting of default

a) Data as per section on Default in Form C will be submitted

b) Creditor may upload/ submit any supporting documents as proof of default along with the data of default

5) Submission of **balance sheet & cash flow statement**: the debtor or its authorised Auditor can submit audited balance sheet and cash-flow statements as electronic documents (PDF, scanned documents etc.)

a) This will be submitted with reference to debtor unique identifier (i.e. PAN)

b) Such submissions can be made directly to the IU

c) Alternatively, IU may consider porting such statements already submitted by the debtor or its Auditor to MCA in digitally signed mode, thereby avoiding the need for direct submission to IU

6) Submission of other **information by IRP**

a) The IRP must be a registered person like any other submitter of information

b) IU should check the IRP has a valid registration number issued by IBBI. This should be validated using an API provided by IBBI.

c) Based on court order documentation made available to IU, the IU will link a debtor to an IRP. The consent framework could be another route for the IRP to get access to the records of the debt in the IU.

d) All submissions of IRP will be with reference to debtor unique identifier

e) Submissions by IRP will be in the form of various documents related to the debtor. Basic metadata about each submitted documents will be submitted along with such documents.

7) IUs can allow multiple modes of submission covering batch upload of multiple records (e.g. manual upload of file or automated server to server file transfer using SOAP based API service or push from creditor's server to a designated SFTP server) or even screen based entry of one record at a time.

8) **Periodic updates** to the financial information can be provided in same Form C format as used for the original information submission since this approach may be easier for various submitting parties. Banks/creditors may find it difficult to submit only incremental changes since the last submission and also such information may only give a partial information to authenticating parties.

9) **Exception handling**: submitted information will be rejected by IU if

a) One or more records of a bulk submission file found not conforming to the specified format or missing mandatory fields

b) Digital signature is found missing, invalid or expired

10) **Error correction**: If any information is noticed to be erroneous, whether before or after it is authenticated, the submitting party should mark the record as erroneous giving reasons and also arrange for corrected data submission as a new update record. Only the submitting party and no other party will be permitted to mark information erroneous. Any user

registered under the submitting party, where a legal entity, will be allowed to mark information submitted by the same legal entity as erroneous.

11) Issuing of **acknowledgement**:
   a) Acknowledgement will be issued on receipt of the valid submission without waiting for authentication to be performed. This will be sent to the registered and verified email ID of the submitting party.
   b) Acknowledgement should specify key information submitted, including receipt date, unique identifier allotted by IU as applicable, terms & conditions of authentication and verification.
      i) Terms and conditions for authentication and verification should contain IU's plans and means of approaching the concerned parties for obtaining authentication.
   c) Submitting user should be able to download, if needed, the acknowledgement as a PDF digitally signed by IU, at any point of time.

***

D. Section IV Authentication and Verification of Information

13(2)(g) Authentication of information
13(2)(h) Verification of information

The standards for authentication and verification for information should cover the following:

1. Facilitating authentication of information from all concerned parties is a core function of an IU.
2. IU should present information to the concerned parties, for verification and authentication by affixing digital signature, based on the information received from submitter, without any changes.
3. IU is required to maintain status of authentication for each record of information including any dispute
4. IU should preserve each artefact used during submission and authentication in its original form as used during digital signature, for the purpose of checking veracity at any time.
5. On authentication of default, IU must inform all related parties to the debt and also all creditors related to the debtor.

Technical Standards 13(2)(g) & 13(2)(h)

1. When a link for authentication is presented by an IU, the party concerned will need to register first if not done already and then proceed with verification and authentication of the information. Individual persons need to be verified against their Aadhaar credentials.

2. Any registered user, on logging into/ accessing the IU portal, will be presented with all pending authentication requests in the relevant section of the portal.

3. The authentication page containing the information will be displayed by the IU to the authenticating person only after verifying identity and credentials of the person from the registration information, whether registered with the same or a different IU.

4. IU must ensure the information presented for authentication is as received in submitted file or extracted from the submitted information, without altering any information elements. The authentication page must contain an undertaking by the authenticating person confirming that he/she has verified the information presented before affixing digital signature/ e-sign. No digital signing should be allowed without presenting the information contained in the underlying data file or document to the authenticating person.

5. When the authenticating party confirms the information and digitally signs the same, IU must ensure that the digital signature is based on and affixed to an artefact (data file/

document) with the same version of the information presented to the authentication party for verification.

    a. For users representing a legal entity, such user is expected to use digital signature certificate (DSC) that has been registered with the IU and linked to the legal entity under the authorised user of the entity or any additional user created under his/her authority and control.

    b. For individuals (e.g. debtor in a retail loan or an individual guarantor), Aadhaar based e-Sign may be used in his/her individual capacity.

6. IU must preserve each piece of data file or document, used for digital signature during submission and authentication, without any alteration so that such artefacts are always verifiable against the digital signature at any point of time in the future to support non-repudiation.

7. When the authenticating party disagrees with or disputes a part or entire information presented, IU should provide for obtaining reason for dispute. Authenticating person's signature will be affixed on the information file which will include dispute flag and reasons for the dispute along with the information presented. IU should notify the submitting party as soon as a dispute is recorded by any concerned party and also make such information available as an exception report.

8. If the authentication request, sent to the concerned party, remains unauthenticated beyond 7 days, the authentication will be considered having 'failed authentication' and the same record will not be available for authentication by the same party subsequently.

9. The different statuses of authentication which need to be maintained by an IU for each record and each party should cover:

    a. '*To be presented*': normally IU will immediately present any received information to the concerned parties for authentication. Hence this status will be transient in nature till a mail/ message is sent out to the concerned parties.

    b. '*Pending authentication*': when the concerned party is yet to undertake authentication.

    c. '*Failed authentication*' if the specified time limit of 7 days is exceeded

    d. '*Authenticated*' when the concerned party verifies, agrees to the information presented and affixes his/her digital signature (or e-Signs) to the information as presented without any change.

    e. '*Disputed*' when the concerned party disagrees / disputes a part or the entire information presented for authentication

10. Authentication status will be maintained in relation to each record of information and each concerned party.

11. If submitted information of default is authenticated by the concerned party or by any third party through any standard mechanism as notified by the Regulator from time to

time, IU will be required to send default confirmation alert to the following along with information of the debt and the debtor.

a. To all parties linked to the defaulted debt (i.e. creditor, guarantors, co-applicants) to the respective registered contact email and mobile numbers

b. To all creditors linked with the same debtor in any other records of debt maintained within the same IU

c. To all other IUs, to allow the each such IU to inform creditors related to debts held by such IU pertaining to the same debtor

***

D. Section V   Standard Terms of Service

13(2)(b) Standard Terms of Service

Technical Standards 13(2)(b)

A. General

1) An IU shall provide the services without discrimination between users.
2) It shall not deny services to any person on the basis of place of residence or business or type of personality
3) An IU shall provide qualitative and error free services to its Users
4) The terms and conditions covering the services and fee structure for its various services shall be informed by the Information Utility upfront to the user and also displayed on its website
5) IU shall charge uniform fee for providing the same service to different users
6) Any change in the fee structure shall be notified to the user at least 3 months before the effective implementation date
7) An IU shall put in place suitable Grievances Redressal Mechanism operated on an electronic platform and ensure prompt redressal of grievances
8) Provide services to a user based on its explicit consent

B. User Registration

1) IU shall verify the Identity of the users registering with it.
2) On registration the users shall be given a Unique ID using the technical standards prescribed by IBBI and communicate the same by email to the Users.
3) IU shall do a deduplication with other IUs and within its database and can deny registration if the user is already registered

C. Submission of Information

1) All information submitted shall be through electronic mode only.
2) The format for capturing the information may include the details as required under Form C or with modifications as required by the IU.
3) On receipt of information submitted by the user and on authentication, the IU shall send an acknowledgement to the user of receipt of the information with specific ID numbers of the Debt / Record
4) Only the original submitters of information shall be allowed to mark erroneous records.
5) IU shall allow only financial information as provided under the Code related to a debt, parties to the debt, security, default etc. to be submitted and stored and deny storing of any other information not related to the above

D. Authentication of Information:

1) The IU shall facilitate the authentication of information through electronic mode duly ensuring that the data is sent to the authorised persons only
2) The IU shall stipulate authentication of information by the Users by using Digital Signature Certificates/e-Sign.
3) IU shall provide the status of information to the submitter of the information;
4) All other users connected to the debt also be permitted to view the status of authentication
5) IU shall take reasonable care in identifying the persons authenticating the information

E. Storage and Access to Information:

1) The financial information collected by an IU shall be stored securely, duly ensuring adequate safeguards and security as prescribed in IT Act
2) Access to data shall be provided only to authorised persons after verifying their identity through log-in credentials
3) Suitable Business Continuity Plan & Disaster Recovery Mechanisms shall be put in place by the IU.
4) Appropriate Security Audits shall be ensured by the Information Utility periodically.

F. Others

1) IU shall provide functionality to access information stored with another IU as per the standards set for interoperability between IUs.
2) Adequate security measures shall be built into such functionality to protect the privacy and confidentiality of information.
3) An IU shall not be responsible for system failures or disruption of service in another IU due to which interoperability is temporarily not feasible.
4) IU shall transfer all the information submitted by a user to another IU on the request of the submitter.
5) IU shall provide every user an annual statement of all information pertaining to that user stored by it, free of charge.
6) IU shall deny registering a user if the verification of ID of the user fails. The user shall be informed of the denial of service.
7) The user shall pay the fee promptly and on non-payment of fee, IU can deny further service.
8) Unauthorised access or unauthorised use of information is subject to civil, criminal, administrative, or other lawful action.

***

D. Section VI   Consent Framework

13(2)(j) Consent Framework for providing access to information to third parties

Technical Standards 13(2)(j)

For **individuals,** the consent artefact should capture the following details:

- Aadhaar number of representative to whom the consent is provided

- Name (as Per Aadhaar)

- Start date of authorization

- End date of authorization

- Reason for authorization

- Consent for Debt Id: Values could be 'ALL' or 'specific' debt numbers (comma separated if multiple debts)

For **legal entities,** the consent artefact should capture the following details:

- PAN number of representative to whom the consent is provided

- Name (as Per PAN)

- Start date of authorization

- End date of authorization

- Reason for authorization

- Consent for Debt Id: Values could be 'ALL' or 'specific' debt numbers (comma separated if multiple debts)

For further details, the MeitY framework document can be obtained from the following link: http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

***

D. Section VII   Data Integrity and Security

13(2)(i) Data Integrity
13(2)(k) Security of the system
13(2)(l) Security of information

The standards related to data integrity and security of system and information should address the following:

1. IT security policy and Cybersecurity policy, detailing all preventive measures to mitigate data security risks, to be put in place
2. The data centre and disaster recovery design and operations to conform to performance standards and operational standards
3. For security standards, IU should consider relevant security frameworks (including cybersecurity) used by regulatory organisations like RBI and SEBI. IU should consider Information Security standards such as ISO 27000 for adoption
4. Business Continuity Plan document of IU should be approved by IBBI
5. IU should establish a robust capacity planning policy
6. Regular security and software audits by Cert-in certified auditors should be conducted
7. Establish efficient information security through SIEM capabilities. The lessons learnt should serve as a policy review tool to prevent recurrence and build safeguards on information assets and infrastructure
8. Building resilience in every sphere of IT function viz., system development, testing, deployment, production monitoring etc., with formal review process to mitigate hidden risks
9. Role and reporting segregation between Chief Technology Officer and Chief Information Security Officer to avoid conflict of interest

Technical Standards 13(2)(i), 13(2)(k) & 13(2)(l)

Information Availability:

1. The IU data centre and Disaster Recovery design and operations should conform to performance standards, such as Uptime Institute's Tier Standards with a data center rating of Tier 3 or above. IU service shall be hosted in a data center and DR facilities within India and shall be governed by the laws of India.
2. Business continuity of IT systems should be ensured through Disaster recovery (DR). IU should put in place a Business Continue Plan (BCP) and get it approved by IBBI. An RPO (Recovery Point Objective) of 15 min and a RTO (Recovery Time Objective) of 1 business day should be adequate considering the nature of IU activity. The same should be reviewed periodically by the IU.
3. A set of policies and procedures should be adopted to enable the recovery or continuation of service following a natural, human-induced disaster or any technological issues

4. To ensure better availability, submission of data simultaneously to both sites can be considered so that data is not lost even if a site goes down before replication can happen.
5. IU should put in place a robust capacity planning policy.

Information Confidentiality:
1. IU service should conform to security standard certification such as ISO 27001. IU should consider adopting security frameworks (including cybersecurity) used in regulatory organisations such as RBI and SEBI. Such standards should be put in place in a graduated manner over next two years or as directed by IBBI.
2. The data should be transferred using secure, authenticated and industry-accepted encryption mechanisms to avoid malicious users intercepting the data and gaining unauthorized access
3. IU should establish adequate security systems to protect the data processing systems against unauthorised access, alteration, destruction, disclosure of information. Encryption of stored data to be considered, may be restricted to more sensitive columns
4. Suitable access control measures to be put in place to prevent unauthorised access to any internal or external persons
5. The Data Centre and DR design should include multi-tier security features like access control to only authorized personnel with proper approval mechanism, audit log for support/service engineers and video monitoring.
6. Since application is exposed to internet, application security testing should be ensured. Application should be tested for security vulnerability. Secure coding standards must be enforced to ensure that such vulnerabilities are not created in the first place and audit of the code should be undertaken to ensure the same.
7. Adherence to the best security practices, with regular security audits by enlisted auditing firms that may be empanelled or that conform to some minimum standards. IU should submit reports of system and IS audit to IBBI.
8. Secure data access should be enabled through *sftp* for bulk transfer and *https* for browser based access
9. Network security should be enforced using Firewall, Intrusion Detection/Protection System, Anti-bot, Antivirus/ Anti malware/ Anti-Spam

Information Integrity:
1. Change Management policies for software releases should be enforced
2. Verification of the identity of the person registering through generally accepted, easily verifiable and reliable sources such as Aadhaar, PAN ID issued by government agencies before allowing the registration. Before registering a user, IU shall ensure that the same user is not registered in any other IU.
3. Email address and mobile number should be verified.
4. Validation of the record of debt in the system of IUs to ensure that every debt record is unique before it is stored in an IU.
5. IU shall accept only digitally signed data/information from the submitter. The digital signature shall be Class 2 or above

6. All information artefacts (data/documents) submitted to the IU shall be stored in the original form for any future reference or verification
7. IU systems should maintain Audit Trail of users, such as IP address, date and time of access

<p align="center">***</p>

D. Section VIII   Risk Management

13(2)(m) Risk Management Framework

Regulatory Context

The Regulations expect the IUs to put in place robust risk management mechanisms to manage the risks embedded in the operations of the IU.

Regulation 13 which states that the Board may lay down standards, through guidelines, for different matters which are all pointers towards risk management.

Regulation 15 mandates every IU to have bye-laws consistent with the code and inter-alia providing for risk management.

Risk management is "a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives" (Institute of Internal Auditors, Florida)

Key considerations

Operational Risk revolves around People, Processes & Technology. Yet in a technology based entity like an IU the accent is expectedly more on the risks revolving around the IT systems.

Broad Draft Technical Standards for Regulation 13(2)(m)

The risk management framework should

1. Define processes to identify, assess, and manage all the risks that may affect the activities of the IU;
2. Encourage high level of accountability across the organisation;
3. Put in place open and transparent communication across the entire organisation; and
4. Clearly identify persons responsible for managing the risk and controls in place.

Detailed Draft Technical Standards for Regulations 13(2)(m)

1. Identification of risk
   a. The objectives of the organisation have to be clearly stated
   b. All potential risks affecting the various operations/services should be identified.
   c. External factors affecting the objectives of the organisation like technological changes/ obsolescence, regulatory changes, risks embedded in outsourced services/vendors etc should be considered
   d. Internal risk factors at the organisational level including interruptions in IT systems, man-made or natural disasters affecting the operations shall be considered
   e. Employees should be encouraged to report incidents, however small they are, to enable to build up data of incidents which will be useful in identifying the risks.

2.   Assessment of Risk
   a. Assess the identified risks as to what will be the impact if that risk has to occur through probability and impact study.
   b. The risks have to be assessed based on the likelihood and impact on the objectives of the organisation
   c. Impact of the risk on earnings, reputation, business and legal implications have to be assessed
   d. Assessed risks may be rated as Low, Medium or High depending upon the probability and impact.

3.   Managing the risk

   a. Risks that cannot be shared, transferred or avoided shall be managed
   b. Decision to share the risk to be decided e.g insurance
   c. A risk register to register various risks under People risk, Operational or Process risk, IT risk, Compliance risk etc. may be prepared.
   d. For managing People Risk, an IU should initiate steps to enforce a culture of integrity & honesty, monitoring work, providing training/retraining for enhancing skills, etc.
   e. For managing Process Risk, an IU should initiate steps to engage professionals to make an independent assessment of risk within the systems & procedures in order to standardise and de-risk procedures and improve systems through improvements and institute appropriate controls.
   f. For managing Technology Risk, an IU should put in place
      o   Reliable, recoverable and secure systems,
      o   Robust Access Control Systems for Data Security,
      o   Network intrusion prevention Systems,
      o   Business Continuity Plans by establishing Disaster Recovery Centre/Near Data Centre,
      o   Getting the VAPT (Vulnerability And Penetration Testing) Tests done at periodical intervals,
      o   Systems Audit done by external auditors on its IT Framework/interface,
      o   Information Security Audit
      o   Adopting Quality Standards and getting Quality Standards Certifications / ISO Standards Certifications done etc.
   g. Risk should be managed by persons close to the risk e.g. unit head, business head, CTO/CISO etc.
   h. Controls should be tested on a periodic basis to ensure effectiveness of the controls
   i. Findings of Audits to be placed before the Board of Directors of the IU which has the overall supervisory responsibility and ensures that proper risk management practices are implemented;

4.   Responsibility in risk management
   a. The CEO has the overall responsibility and ensures that every employee of the organisation is aware of risks affecting the operations
   b. Senior management of the organisation shall put in place risk management policy and processes containing the organisation's view on risks and identifying various risks like operational risk, IT risk, Compliance risk and controls for the same; also they should review the risk management process on regular intervals;

5.   Monitoring the risk management process

   a. IT security systems and processes shall be audited by a CISA qualified external auditor
   b.   The Regulatory committee may supervise the compliance risk and the external Risk Auditor shall give its report to the Regulatory Committee.
   c.   The CEO shall report to the governing board on a quarterly basis the functioning of risk management and exceptions found if any;
   d. Audit committee, in the absence of a risk committee, may review the IT audit report to ensure that the controls are functioning effectively

***

D. Section IX   Preservation and Purging of Information

13(2)(q) Preservation of Information
13(2)(r) Purging of information

Technical Standards 13(2)(q) & 13(2)(r)

1. All information maintained by an IU will be in electronic form only.

2. IU can choose its internal data store design and data format. However, such storage format should not inhibit exchange or transfer of data between IUs or inter-operability of IUs in any manner.

3. Any artefact, in the form of data file or scanned /other documents, which are digitally signed by a user of an IU, must be preserved in the original form which was used for digital signature. This is to ensure that the digital signature is verifiable with the document anytime in the future.

4. Digital signature should be stored with the information file where embedding is allowed (e.g. PDF, XML formats), or separately such that the information file corresponding to the signature can be easily identified to facilitate verification by an independent person.

5. All information, including any supporting documents, stored and preserved by IU must be linked to clearly identifiable unique records of information (e.g. UDI) or person.

6. No financial information stored in an IU will be deleted or modified. Any update to information will be added as a new information record. All old records will be preserved till purged after the specified period of time.

7. If and when permitted by the Regulatory standards or notification, an IU may be allowed to store reference links to external registries (e.g. CERSAI) to enable IU to fetch and retrieve related records/ documents on need basis to service user requests of information retrieval, without the need to import and replicate the entire database of such registries. Such import mechanism shall be addressed in further detail in the 2nd Part of the Report

8. Similarly, for servicing any information requests related to information stored at other IUs, an IU can retrieve such information on need basis as per allowed norms of inter-operability of IUs as shall be laid down in the 2nd part of the Report

9. IU is required to maintain and preserve audit trail of all usage of information, including submission, authentication and information retrieval activities for each user

    1. Minimum information to be maintained as audit trail for financial information will cover at least the user ID, date and time, type of service used and record ID

    2. In addition, IU should maintain audit trail of other non-financial information such as user administration/ system access e.g. user creation, deletion,

activation, change of user access privileges, change in user profiles including upload of DSC, login, session duration, unsuccessful login attempt etc.

10. IU should maintain backup of all financial information stored with it periodically in offline media storage to guard against possible data corruption of its online storage/ servers

    1. Such media storage should be preserved in a secured manner to prevent unauthorized access or damage

    2. IU should carry out periodic verification to check that the data on the media is restorable

11. Duration of preservation and Purging of data: Keeping with the generally accepted period of storage of public documents of 5 to 8 years, it is recommended that an IU preserves old records for a period of 8 years from the date of closure of loan

    1. Considering that an IU will not maintain a loan account with its status in a way the creditor does and that information maintained about a loan is in the form of a series of updates, each appended as new record, a closure of loan in this context will imply records of debt which have stopped receiving any updates.

    2. An IU may permanently delete records of debt where last update date is earlier than 8 years.

    3. IU will maintain a metadata about the purged records including UDI, creditor ID, debtor ID, other party IDs, last updated date and date of purging

***

E. Annexure: Description of fields in Form C

A - 1. Submitter Information

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
1	Submitter's Unique Identifier Number (UIN) allotted by IU	Text	PAN No. for legal entity & AADHAAR No. for individuals	Y	
2	Submitter's name	Text	Formal name (First +Middle+Last) without salutations	Y	
3	Relationship of submitter to the Debt	LoV	'Creditor', 'Debtor' 'Guarantor' etc	Y	Will be 'Creditor' in most cases. But can be a 'Debtor' or 'Guarantor' in some situation

4	Date of Incorporation (Legal Entity) / Date of Birth (Individuals)	Date	As declared	Y	For registered submitter, will be picked from registration data. Need not be part of data file
5	Communication address of submitter	Text		Y	For registered submitter, will be picked from registration data. Need not be part of data file
6	PIN code of submitter	LoV	Valid PIN code from list (communication)	Y	For registered submitter, will be picked from registration data. Need not be part of data file

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
7	Telephone number	Text	With ISD country and STD area code	Y	For registered submitter, will be picked from registration data. Need not be part of data file
8	Mobile number	Text	With ISD country code	Y	For registered submitter, will be picked from registration data. Need not be part of data file
9	Email ID	Text		Y	For registered submitter, will be picked from registration data. Need not be part of data file

A-2. Other Party Information (Repeat field set for each party)

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
10	Relationship to debt	LoV	Debtor', 'Creditor', 'Guarantor' 'Co-applicant', Co-obligant' etc	Y	Other party to be different from the submitter. If submitter is creditor, other party cannot be a creditor
11	Counterparty name	Text	As per submitter (First+Middle+Last without salutations)	Y	
12	Registered/ permanent Address of counterparty	Text	Registered office address for legal entity Permanent address for Individuals	Y	

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
13	PIN code (Regd. Office)	LoV	Valid PIN code from list (registered/ permanent)	Y	
14	Address for Communication	Text	Current Communication address	Y	
15	PIN code (Comm. Address)	LoV	Valid PIN code from list (communication)	Y	
16	Legal Constitution	LoV	Public Ltd Co/ Pvt Ltd Co / LLP / Partnership/OPC/Resident Individual/ Non-resident/Foreign	N	Needed for validation of type of ID to be checked
17	Date of Incorporation (Legal Entity) / Date of Birth (Individuals)	Date	As declared	Y	

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
18	Corporate Identification Number (CIN/LLPIN) for Corporates	Text	For registered legal entities	N	For deduplication
19	PAN No.	Text	For legal entity and also individuals. Mandatory for legal entity other than foreign	N	For identity/ deduplication
20	AADHAAR	Text	Mandatory for resident individuals.	N	For identity/ deduplication
21	Counterparty Contact Person Name	Text	Contact of representative employee	N	Needed for reaching out for authentication
22	Contact Person's Designation	Text	As per submitter	N	Needed for reaching out for authentication

23	Contact Person's Mobile No.	Text	As per submitter. One of mobile or email mandatory	Y	Needed for reaching out for authentication
24	Alternative Mobile No.	Text		N	
25	E mail id	Text	As per submitter (official email ID)	Y	Needed for reaching out for authentication
26	Alternative Email ID	Text		N	

A-3. Debt Information

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
27	Loan A/c Number	Text	Contract No. for Bills /LC/ Bank Guarantees; & Loan No. for Term Loans and OD/CC (For OC: Invoice No.)	Y	Creditor's loan number, mapped with UDI at IU end
28	Old Account Number (wherever applicable)	Text	Link to the Old account number to maintain history Creditor's PAN (i.e UIN) + old Loan a/c number	N	Audit trail and migration related issues
29	Date of Sanction of Credit Facility	Date	Date of latest renewal for OD/CC limits & Date of sanction for Term Loans (For OC: Date of Invoice)	Y	

30	Date of disbursement or activation	Date	Date of first disbursement for OC: Date of delivery	Y	
31	Currency of loan or exposure	LoV	Applicable Currency Code (e.g. INR, USD)	Y	All amounts in other fields will be in this currency
32	Sanctioned Amount	Number	Amount sanctioned For OC: Amount of Invoice Non-funds based it is the sanctioned limit	Y	
33	Nature of credit facility	LoV	Category code for product - Financial (fund/ non-fund based), Operational, secured/unsecured	Y	
34	Facility name	Text	Free text of product name	N	As known to debtor. To be presented during authentication

35	Repayment frequency	LoV	Monthly, Quarterly, Half yearly, Annual, On demand, bullet, Rolling, Others	Y	Repayment schedule difficult to get from creditors as per feedback
36	Rate of interest	Number	Applicable rate of interest on date of reporting	Y	
37	Lending arrangement	LoV	Sole Banking / Consortium / MBA	N	to link with security and numbers of creditors
39	Total Outstanding Amount	Number	Total outstanding as on the date of reporting including Principal, Interest, Charges etc. (For Fund based Limits); For non-fund based limits, please indicate Contingent Liability; For OC: Amount due under the invoice	Y	

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
40	Amount Overdue	Number	Amount overdue (aggregate of principal, interest, charges etc.) as on date of reporting	N	Data to be used for evidencing default If no overdue, report zero value
41	Days past due (DPD)	Number	Number of days overdue as on date of reporting	N	DPD applicable across all creditors (non-banking, operational etc) - data to be used for evidencing default If no overdue, report zero value

B. Security Information

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
42	Date of creation of charge	Date	As stored by the Creditor	Y	Mandatory where security record submitted
43	Type of Charge created	LoV	Indicate whether it is: Mortgage / Hypothecation / Charge / Assignment / Pledge / Lien / Negative Lien	Y	Mandatory where security record submitted

| 44 | Assets typ | Text | Free text description of asset type over which charge created (Movable/ immovable/ intangible etc.) | Y | Mandatory where security record submitted Illustrative list: Cash / Bullion / Bank Deposits NSCs/KVPs LI Policies Shares/Bonds/Securities Inventory (Raw Materials, WIP & Finished Goods Accounts Receivables Other Current Assets (Indicate whether Raw Materials/Stocks in Process / Finished Goods; Book Debts etc.) Plant & Machinery / Equipment Land & Buildings Vehicles Other Fixed Assets Other Movable Assets |

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
46	Description of security	Text	Any description or details like number, identification marks etc.	Y	To facilitate authentication of security. Other fields do not provide sufficient information to identify security
47	Value of security	Number	Value of asset over which charge is created	Y	Mandatory where security record submitted
48	Date of valuation	Number	Date of valuation report for immovable properties & Date of Stock Statement for Stocks & Book Debts	Y	Mandatory where security record submitted
49	Security Classification	LoV	Primary or collateral	Y	

50	Security Interest ID with ROC		As available with the creditor	N	
51	Security Interest ID as per CERSAI		As available with the creditor	Y	

C. Default Information

Sl. No.	Field Name	Fld Type	Description of the field	Form C (Reg)	Remarks
52	Loan A/c Number	Text	Loan account on which default is reported	Y	Creditor's loan number, mapped with UDI at IU end
53	Date of default	Date	Due date for payment;	Y	
54	Total Outstanding	Number	Total outstanding as on the date of reporting including Principal, Interest, Charges etc.	Y	
55	Default amount	Number	Amount fallen due but not paid	Y	
56	Days past due	Number	As on date of reporting default	Y	
57	Amount of last repayment	Number		Y	
58	Date of last repayment	Date		Y	

59	Date of filing of suit	Date	Date of filing of suit by the Creditor against the Debtor	N	Required for Operational creditors if available. Not required for banks
60	Supporting documents	Attachment	Attach documents such as repayment schedule, account statement, any supporting documents for proving default	Y	

F. Order for Constitution of the Technical Committee

3rd May, 2017

Order

Sub: Constitution of Technical Committee under the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017

In pursuance of the provisions of Regulation 14 of the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017 (Regulations), a Technical Committee is constituted as under:

    a. The Technical Committee shall consist of the following:

Sl. No	Name and Position	Position in Committee
	Dr. R. B. Barman (Chairman, National Statistical Commission)	Chairperson
	Dr. Nand Lal Sarda (Emeritus Fellow, Indian Institute of Technology, Bombay)	Member
	Dr. Pulak Ghosh (Professor, Indian Institute of Management, Bangalore)	Member
	Sh. V. G. Kannan (Chief Executive, Indian Banks Association)	Member

    b. The Technical Committee shall recommend technical standards required to be laid down by the Board under the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017.

    c. The Technical Committee shall advise and provide professional support, on a request from the Board, and it may advise the Board, on its own volition, on any matter under the Insolvency and Bankruptcy Board of India (Information Utilities) Regulations, 2017.

    d. The IBBI shall designate one of its senior officers as the Secretary to the Technical Committee and such Secretary shall have the right to speak, but not vote on any matter in meetings of the Technical Committee;

2. Chapter III of the Insolvency and Bankruptcy Board of India (Advisory Committee) Regulations, 2017 shall apply mutatis mutandis to the Technical Committee.

3. The term of a member in the Technical Committee is two years or until further orders, whichever is earlier.

                                                 - Sd -
                                        (Anita Kulshrestha)
                                  Deputy General Manager

To
1. Dr. R. B. Barman, Chairman, National Statistical Commission
2. Dr. Nand Lal Sarda, Emeritus Fellow, Indian Institute of Technology, Bombay
3. Dr. Pulak Ghosh, Professor, Indian Institute of Management, Bangalore
4. Sh. V. G. Kannan, Chief Executive, Indian Banks Association
5. PS to Chairperson, IBBI
6. Ms. Suman Saxena, Whole Time Member, IBBI
7. Dr. Navrang Saini, Whole Time Member, IBBI
8. Dr. Mukulita Vijayawargiya, Whole Time Member, IBB