

Real Time Gross Settlement System Regulations

Version 1.0



Reserve Bank of India
Department of Payment & Settlement Systems
Central Office, Mumbai

Version Control

Version	Date	Description/Changes
1.0	October 21, 2024	<p>Following changes were incorporated/updated in RTGS System Regulations 2013:</p> <ol style="list-style-type: none"> 1. Chapter 3 – Management of RTGS <ol style="list-style-type: none"> a. Constitution of the standing committee 2. Chapter 4 - Membership <ol style="list-style-type: none"> a. Updated list of eligible entities b. Updated access criteria for accessing RTGS c. Updated process for applying for membership d. Updated type of memberships e. Deleted para 4.7 of existing regulations f. Introduced para on withdrawal of membership g. Introduced para on review of membership 3. Chapter 10- Rights of Members/Participants <ol style="list-style-type: none"> a. Deleted para on withdrawal of membership 4. Chapter 11 – Customer Transactions <ol style="list-style-type: none"> a. Introduced description format for account statement 5. Chapter 13 – Obligations and Duties of Members/Participants <ol style="list-style-type: none"> a. Introduced requirements related to LEI b. Introduced requirements related to FCRA c. Updated instructions regarding membership fee 6. Chapter 14 – Sub-membership in RTGS <ol style="list-style-type: none"> a. Updated eligibility for becoming sponsor/sub-member b. Introduced instructions regarding reporting to

		<p style="text-align: center;">CPFIR</p> <ol style="list-style-type: none"> 7. Introduced new chapter: “Chapter 17 – Cyber Security Guidelines for RTGS” along with Annex 10 specifying baselines cyber security controls 8. Introduced application form for approval for membership for Centralised Payment Systems at Annex 11 9. Incorporated instructions issued vide various circulars on RTGS.
--	--	---

Table of Contents

Chapter No.	Chapter	Page
Chapter – 1	Scope and Objective	6
Chapter – 2	Definition of Terminology	7
Chapter – 3	Management of RTGS	9
Chapter – 4	Membership	12
Chapter – 5	RTGS Transaction Type and Message Formats	19
Chapter – 6	Components, Communication and Settlement	20
Chapter – 7	RTGS Business Day and Operating Sessions	23
Chapter – 8	Intra-day Liquidity (IDL) Facility	25
Chapter – 9	Other Features of RTGS	27
Chapter – 10	Rights of Members / Participants	28
Chapter – 11	Customer Transactions – Obligations and Rights of Members / Participants	29
Chapter – 12	MNSB Settlement and Clearing House Participants	32
Chapter – 13	Obligations and Duties of Members / Participants	34
Chapter – 14	Sub-Membership in RTGS	37
Chapter – 15	Dispute Resolution and Miscellaneous	39
Chapter – 16	Disclosures	41
Chapter - 17	Cyber Security Guidelines for RTGS	42
Annex – 1	Transaction Type, Message Formats and Major Rules	43
Annex – 2	Channel Codes for UTR / Transaction identifications	44
Annex – 3	Codes on Message Validation (RTGS)	45
Annex – 4	List of TTC Values and Priority for RTGS	47
Annex – 5	Cut-off Times in the RTGS at RBI	48
Annex – 6	RTGS Threshold Value and Maximum Service Charges for Customers	49
Annex – 7	Capturing Legal Entity Identifier in RTGS Message	50

Annex – 8	FCRA related transaction code in RTGS Systems	51
Annex – 9	RTGS Service Charges for Members	52
Annex – 10	Baseline Cyber Security Guidelines for RTGS	53
Annex – 11	Application Form for Approval for Membership of Centralised Payment Systems	56

Chapter – 1

Scope and Objective

1.1 With the advent of new technology, it being necessary and expedient to set up a Real Time Gross Settlement (RTGS) system for facilitating on-line real time settlement of payments, the Reserve Bank of India (RBI / the Bank) has setup a RTGS system and has framed these regulations for matters connected therewith or incidental thereto.

1.2 Short title and commencement

(1) These Regulations may be called RTGS System Regulations.

(2) They shall come into force from the date of their Notification under the Payment and Settlement Systems Act, 2007 and Payment and Settlement Systems Regulations, 2008.¹

1.3 Extension of timings

Operating hours of RTGS were extended for customer and inter-bank transactions at different points of time and has been made available round the clock on all days of the year with effect from December 14, 2020.

¹ RTGS (Membership) Business Operating Guidelines, 2004, RTGS (Membership) Regulations, 2004 and RTGS System Regulations, 2013 shall cease to exist.

Chapter – 2

Definition of Terminology

- (i) 'Access Criteria for payment systems' means a set of criteria / norms issued by RBI from time to time to allow a member to access the Payment Systems.
- (ii) 'Ancillary Payment System' means a payment system operated by RBI or any Clearing Entity. For example, paper (CTS) clearing, NEFT, CCIL, NPCI operated systems and systems operated by SEBI regulated clearing entities, etc.²
- (iii) 'Bank' means the Reserve Bank of India.
- (iv) 'Central System' means the hardware and software installed in a central location hosting RTGS application to process and settle funds transfer requests received from the members. The Central System shall be operated and managed by the Bank.
- (v) 'Centralised Payment System' means and includes Real Time Gross Settlement (RTGS) System, National Electronic Funds Transfer (NEFT) System and any other system as may be decided by RBI from time to time.
- (vi) 'Customer transaction' means a funds transfer originated or received by a member on behalf of its customer.
- (vii) 'e-Kuber' means Core Banking Solution of the Bank maintaining current accounts of the banks, Governments and other institutions / entities.
- (viii) 'Host system' means members own system like Core Banking Solution (CBS) system or a similar kind of application.
- (ix) 'INFINET' means the Indian Financial Network, the communication backbone.
- (x) 'Inter-institutional transaction' means a funds transfer between two RTGS System members / participants.
- (xi) 'Interface' means the utility (software application) which helps the interaction between a member's host system and the Member Interface of RTGS.

² The acronyms stand for (i) MICR – Magnetic Ink Character Recognition; (ii) CTS – Cheque Truncation System; (iii) NEFT – National Electronic Funds Transfer; (iv) NECS – National Electronic Clearing Services; (v) CCIL – Clearing Corporation of India Ltd.; (vi) NPCI – National Payments Corporation of India; and (vii) SEBI – Securities and Exchange Board of India.

(xii) 'Intra-day Liquidity (IDL)' means the liquidity support provided by the Bank during a RTGS business day to the members against eligible collateral.

(xiii) 'Member' means an entity admitted by the Bank to access RTGS.

(xiv) 'Member Interface (MI)' means the hardware and software component installed at the member's / participant's end connecting with the Central System.

(xv) 'Multilateral Net Settlement Batch (MNSB)' means a settlement file containing the net funds positions (receivable / payable) of clearing members emanating from various payment systems having current account / settlement account with the Bank.

(xvi) 'Own Account Transfer' means transfer of funds between member's current account and settlement account maintained with the Bank.

(xvii) 'RTGS' system means system which facilitates on-line real time settlement of payments either on gross basis or through Multilateral Settlement Batches, received from the members.

(xviii) 'Settlement Account' means an account opened with the Bank by members of RTGS to facilitate settlement of transactions.

(xix) 'SFMS' means the Structured Financial Messaging Solution provided by Indian Financial Technology & Allied Services (IFTAS).

(xx) 'SWIFT' means the messaging system provided by the Society for Worldwide Interbank Financial Telecommunication.

(xxi) 'System Operator' means the Bank which shall operate and manage the Central System.

(xxii) 'UTR Number / Transaction Identification' means Unique Transaction Reference Number that identifies a transaction uniquely.

Chapter – 3

Management of RTGS

Operations of RTGS

3.1 RTGS shall be operated by the Bank under the supervision of the Regional Director, Reserve Bank of India, Mumbai Regional Office, Shahid Bhagat Singh Marg, Fort, Mumbai 400 001.

3.2 A Standing Committee on Centralised Payment Systems shall be constituted for management of RTGS/NEFT system so as to provide a structured forum for continuous dialogue with the members. Its role is to provide inputs to RBI for improvement and smooth functioning of RTGS/NEFT.

3.2.1 Governance: Constitution of Standing Committee

I. The composition of the standing committee shall be as under:

- a. President – The Regional Director, Mumbai Regional Office (MRO), RBI, Mumbai.
- b. Representatives from Department of Payment and Settlement Systems (DPSS), CO, RBI, Mumbai; Department of Information Technology (DIT), CO, RBI, Mumbai and Department of Government and Bank Accounts (DGBA), CO, RBI, Mumbai.
- c. Two Representatives from other stakeholder RBI departments on rotation – Internal Debt Management Department (IDMD), CO, RBI, Mumbai; Consumer Education and Protection Department (CEPD), CO, RBI, Mumbai; Financial Markets Operations Department (FMOD), CO, RBI, Mumbai; Department of Regulation (DoR), CO, RBI, Mumbai; Department of Supervision (DoS), CO, RBI, Mumbai; Foreign Exchange Department (FED), CO, RBI, Mumbai; Monetary Policy Department (MPD), CO, RBI, Mumbai and Legal Department (LD), RBI, Mumbai.
- d. Representatives from Member Institutions (officer of Deputy General Manager or equivalent level and above):
 - i. Nationalised Banks – State Bank of India (SBI) and one other

- ii. One Private Bank
- iii. One Foreign Bank
- iv. Two from other bank categories - Co-operative Banks / Payment Banks / Small Finance Banks / Regional Rural Banks.
- v. One Primary Dealer
- vi. Clearing Houses - Clearing Corporation of India Limited (CCIL), National Payments Corporation of India (NPCI) and one Securities and Exchange Board of India (SEBI) approved participant.
- vii. One Authorised non-bank Payment System Operator (PSO).

II. The secretarial assistance to the Standing Committee shall be provided by DPSS, MRO, RBI, Mumbai.

III. The President, representatives from DPSS CO, DIT CO, DGBA, SBI, NPCI and CCIL shall be permanent members. Other members shall be replaced on a rotation basis every two years.

IV. The committee may constitute ad-hoc sub-committees to consider specific aspects, as and when required.

3.2.2 Meeting of the committee

- a. The committee may meet on a need basis, but at least once every half-year.
- b. The quorum for meeting may comprise of the President, members listed in 3.2.1.I(b), not less than one member listed in 3.2.1.I(c), and not less than three members listed in 3.2.1.I(d).

3.2.3 Functions of Standing Committee

The functions of the Standing Committee shall include the following in relation to the RTGS systems:

- a. Gathering feedback from industry, examining suggestions and recommending policy improvements to DPSS, CO, RBI, Mumbai.
- b. Coordinating steps taken by stakeholders in alignment with regulations issued by RBI and Centralised Payment Systems (CPS) related goalposts laid down in the RBI Payments Vision documents.

- c. Monitoring various operational and security aspects viz. business continuity management (BCM), cyber resilience of participants' systems, information security, availability of sufficient funds for settlement, 24x7 availability of systems, etc.
- d. Matters relating to customer protection and enhancement of customer experience in RTGS.
- e. Any such issues, as it may deem fit and proper for the smooth, satisfactory and proper functioning of RTGS.

Chapter – 4

Membership

4.1 Membership of RTGS shall be open to all scheduled/licensed banks, standalone primary dealers, PPI issuers, white label ATM operators and card networks.

4.2 For clearing organisations, other categories of Payment System Providers (PSPs) and other entities, RBI shall consider membership requests on a case-to-case basis.

4.3 Cooperative societies and unlicensed banks can not become member of the RTGS.

4.4 The Bank at its discretion may permit other entities to become members of RTGS.

Criteria for Membership

4.5 The applicant entity shall meet the following criteria for becoming a member of RTGS:

- a) Entity should hold valid license/authorization/registration from the concerned financial regulator;
- b) Entity should operate on core banking solution / centralised processing system;
- c) Entity should have adequate technical competence and system readiness including cyber resilience;
- d) Entity should be in compliance with the guidelines on storage of payment system data;
- e) Entity should be in compliance with baseline cyber security guidelines given at Annex 10.
- f) Non-bank Payment System Providers (PSPs) should be incorporated in India under the Companies Act, 1956 / 2013. Authorised non-bank PSPs incorporated outside India shall empower their local subsidiary/associate to enter into valid agreement with RBI as well as to carry out all operations pertaining to the payment system. The responsibility for all operations and

management of any contingency, including settlement obligations, shall remain with the parent institution, which has been granted authorisation as a PSP; and

- g) Non-bank PSPs should have a satisfactory record of compliance to the conditions laid out in the Certificate of Authorisation (CoA) and regulatory guidelines issued by RBI.

4.6 The entities shall also meet the following financial criteria to become a member:

Type of Entity	Criteria
Scheduled/Licensed Banks	a) Adherence to current CRAR requirements stipulated by the RBI; b) Net NPA below 5% (as per the latest audited balance sheet); and c) Minimum net-worth prescribed by RBI or ₹25 crore, whichever is higher.
Authorised non-bank PSPs	Minimum net-worth prescribed by RBI or ₹25 crore, whichever is higher.
Standalone Primary Dealers	a) Minimum net-worth prescribed by RBI or ₹25 crore, whichever is higher; and b) Adherence to CRAR requirements stipulated by the RBI.

4.7 To access RTGS, an entity shall need to meet with the other specific requirements, as may be advised. These may include:

- (i) Membership of the Indian Financial Network (INFINET) / SFMS
- (ii) Maintaining a current account with the Bank.
- (iii) Maintaining a settlement account with the Bank.
- (iv) Maintaining Subsidiary General Ledger (SGL) account with the Bank.
- (v) Any other additional requirements specified by the Bank.

4.8 The Bank at its discretion may amend the access criteria from time to time.

Process for Applying for the Membership

4.9 An entity eligible under above guidelines for RTGS can apply for approval for membership of Centralised Payment Systems in the format prescribed at [Annex 11](#)

along with required documents. The application should be submitted to the Chief General Manger, Reserve Bank of India, Department of Payment and Settlement Systems (DPSS), 14th Floor, Central Office Building, Shahid Bhagat Singh Marg, Fort, Mumbai – 400 001. The application can also be submitted through the Pravaah portal of RBI which can be accessed at <https://pravaah.rbi.org.in>.

4.10 Approval for membership shall be subject to favorable supervisory / regulatory recommendation as well as approval from other stakeholder departments of RBI. The recommendation of the regulatory/supervisory/stakeholder departments/organisations shall be obtained independently and need not be furnished by the applicant at the time of submission of the application.

4.11 Recommendation of the regulatory / supervisory department/organisation is not required for newly licensed banks if the bank has submitted its application for Centralised Payment Systems before starting to provide services as bank.

4.12. In case the application is favourably considered, an in-principle approval for the membership shall be granted to the applicant entity. Entity shall also be granted a unique primary Indian Financial System Code (IFSC) to be used for RTGS/NEFT. The approval letter shall indicate the type of membership, types of transactions it is permitted to undertake, facilities available, etc. In case the request is declined, the applicant shall be advised the reason(s) for which the membership has not been considered.

4.13 Applicant entity shall be given a timeline, as specified in the in-principle approval for membership, to operationalise RTGS membership. In case the entity is unable to ensure participation in RTGS within the specified period, it will need to apply for extension of approval. RBI will ascertain genuineness of request and provide extension up to one year from the date of issuance of initial approval letter.

4.14 After receiving in-principle approval for RTGS membership, the entity shall approach the Regional Director, Reserve Bank of India, Mumbai Regional Office, Main Building, Shahid Bhagat Singh Marg, Fort, Mumbai 400 001 for completion of necessary documentation and operational clearances.

4.15 After setting up the necessary infrastructure for participation in RTGS and completion of User Acceptance Testing, the applicant shall get conducted an information systems audit of the RTGS related systems by a CERT-In empaneled IS

auditor. The applicant shall also obtain a certificate from a CERT-In empaneled IS auditor confirming compliance with baseline cyber security guidelines for RTGS (given at [Annex 10](#)). On receipt of IS audit report along with compliance (with no pending major IS audit observations) and on verifying readiness, RBI shall grant approval for go-live. The newly licensed banks applying for RTGS membership shall also need to show compliance with the access criteria before go-live in RTGS.

4.16 Entities not seeking access to RTGS/NEFT but desirous of opening only a current account, SGL/Constituent SGL (CSGL) account, INFINET membership, NDS-OM and NDS-Call membership shall directly approach the concerned regional office / central office department of RBI.

Type of membership

4.17 There are four types of participants in RTGS viz., (i) Central Bank – exclusively for the Bank (ii) regular participant – all types of facilities to be provided (e.g. banks), (iii) restricted participant – some particular type(s) of facilities to be provided (e.g. Primary Dealers) and (iv) clearing house – permitted to submit MNSB file to RTGS.

4.18 The existing RTGS participants are mapped to the new RTGS as follows:

Sr. No.	Membership Type	Broad Category	Entities	Facilities available
1.	Type A	Regular Participant	Scheduled/Licensed Banks	IDL, inter-bank, customer transactions, own account transfer
2.	Type B	Restricted Participant	Standalone Primary Dealers	IDL, inter-bank, own account transfer
3.	Type C	Clearing House	Clearing Houses, Card Networks	Gross transaction, MNSB, any other transactions / facilities approved by the Bank.
4.	Type D	Regular or Restricted Participant or clearing house	Non-bank Issuers, PPI WLA operators	Customer Transactions, Inter-bank, IDL/No IDL, Own Account Transfer, any other conditions applied by RBI

The facilities mentioned above are indicative. The Bank has the right to change these facilities for any particular participant, if necessary. The Bank may define new membership types or disable an existing membership type at any point of time.

4.19 Non-bank PSPs shall not be eligible for availing Intra-Day Liquidity (IDL) facility from the Reserve Bank. For any shortfall / default in completing the payment / settlement obligations, such entities shall approach their bankers for a ready line of credit facility. They shall ensure that appropriate liquidity support arrangements are in place with their bankers to avoid gridlocks and to ensure business continuity.

4.20 Card networks shall not be allowed to use the RBI current account for their settlement guarantee and related activities.

Options for accessing RTGS

4.21 The members have to opt for any of the three options viz., thick-client, Web-API (through INFINET or any other approved network) and Payment Originator (PO) module. The choice of options for connecting to RTGS is based on volumes and business requirements of a member:

- (a) **Thick client interface / SFMS Member Interface:** A Member has to own, install and maintain the dedicated hardware and software connecting to the Central System through INFINET or any other network approved by the Bank.
- (b) **Web service interface:** The interface application has to be developed by the members as per the specification provided by the Bank. The Central System shall have to be connected through INFINET or any other network approved by the Bank. Necessary specifications and standards for developing the application for web service have been made available on the Bank's website.
(Hyperlink - http://www.rbi.org.in/Scripts/Bs_viewRTGS.aspx)
- (c) **Payment Originator (PO) module:** This is a browser-based mode of access. Members can originate and receive payment transactions through INFINET / any other network approved by the Bank. Participants having daily average volume 100 or less RTGS transactions are permitted to use this mode of access. The Bank reserves the right to revise the average daily transaction limit for accessing RTGS through PO module in future. The Bank shall issue

specific instructions to the members for accessing RTGS through public internet.

4.22 A participant can access the Central System through one channel at a time, which is said to be the primary channel. The preference has to be provided to the Bank for necessary configuration at the Central System. Another access channel shall work as a back-up channel and the member has to inform the Bank mandatorily before switching to another channel.

Withdrawal from Membership

4.23 A participant / member may resign from the membership of RTGS after giving a 30 day prior notice to the Chief General Manager, Reserve Bank of India, Department of Payment and Settlement Systems, Central Office, Mumbai. The Bank shall accept the resignation within the notice period, subject to such conditions, as it deems necessary to impose on the member and the member shall be bound to comply with the said conditions. The resignation shall take effect on acceptance thereof by the Bank.

Review of Membership

4.24 Continued participation of an entity in the centralised payment systems shall be dependent on its continuous adherence to the requirements of access criteria, meeting the cyber security guidelines for RTGS and supervisory comfort. The RBI may place restrictions on a particular member on its participation in these payment systems, penalise, suspend, revoke the membership of an entity if its participation in payment system is found to be detrimental to the smooth functioning of the payment system in any manner.

4.25 To ensure continued adherence to access criteria and cyber security guidelines, members will be required to submit an annual compliance statement to RBI. Annual statement shall include audit report of their RTGS related systems by a CERT-In empanelled IS auditor.

4.26 Apart from annual review, membership may also be reviewed based on other triggers, which may include but not limited to:

- a) Non-adherence to access criteria and cyber security guidelines for RTGS / NEFT at any time;

- b) Failure to manage its liquidity position in payment systems;
- c) Cyber security risks and related incidents;
- d) Supervisory concerns on continued participation in payment systems;
- e) Non-adherence to applicable guidelines of the payment systems; and
- f) Any other changes making entity ineligible for membership.

4.27 Based on the severity of the deviations / risks observed in the review, the member shall be classified into one of the following categories and appropriate action may be taken. The actions given are suggestive. RBI may take any action it considers appropriate. If the entity does not correct the deviation / act on the risk within the time permitted, action as per the next higher category may be initiated.

Category	Description	Action
A	Low deviation / Risk	1. Advisory to be issued to the member
B	Moderate deviation / Risk	1. Seeking explanation from the member 2. Providing appropriate time to fix the issues
C	High deviation / Risk	1. Seeking explanation from the member 2. Placing time or/and transaction type restrictions ³ 3. Mandating earmarking securities for IDL for eligible entities 4. Advising IS audit for IT systems
D	Very high deviation / risk	1. Revoking membership of RTGS / NEFT

4.28 Where a member is subsequently debarred from the payment system or downgraded in access to the payment system, the continuation or otherwise of the other accounts / membership (i.e. current account, SGL / IDL-SGL / CSGL account, NDS-OM and NDS-Call membership, INFINET membership) shall be decided by RBI separately.

³ Depending on the risk, restrictions may be placed on members from originating or receiving RTGS / NEFT transactions during certain times (time restrictions) like from 8:00 pm to 8:00 am or / and certain types of transactions (transaction type restrictions) like outgoing transactions.

Chapter – 5

RTGS Transaction Type and Message Formats

5.1 RTGS shall process following types of transactions:

- a. *Inter-institutional / inter-bank transaction* – Funds transfer between two RTGS members.
- b. *Customer transaction* – Funds transfer / receipt on behalf of a customer of a RTGS member.
- c. *Government transaction* – Funds transfer / receipt on behalf of Government Accounts by a member.
- d. *Multilateral Net Settlement Batch (MNSB)* – The file containing net settlement position of clearing participants of an ancillary payment system managed by a clearing house / payment system.
- e. *Delivery versus Payment (DvP)* – A transaction involving funds in one leg against delivery of securities on the other leg. (A securities settlement mechanism that links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding payment occurs.)
- f. *Own Account Transfer (OAT)* – Transfer of funds by a member between RTGS settlement account and a current account maintained with the Bank.
- g. *Return Payment Transaction* – Credit transfer received by a member through RTGS that could not be credited to an account specified in the message and which is required to be returned to the sending member.

5.1.1 The standard message formats for the transaction types listed above along with major validation rules are at [Annex 1](#).

5.2 The Bank has the right to introduce any other transaction type, if considered necessary.

Chapter – 6

Components, Communication and Settlement

6.1 *Transaction Flow*: Each member shall communicate from its Member Interface to the Central System through the INFINET or any other network permitted by the Bank. The interactions between the Member Interface and the Central System shall be through a pre-defined message format (**ISO 20022**) only. For ensuring security, all messages shall be digitally signed and encrypted. The Institute for Development and Research in Banking Technology (IDRBT), or any other institute as decided by the Bank, shall be the Certifying Authority (CA) for digital certificates.

6.2 *Unique Transaction Reference (UTR) / Transaction Identification Number*. Each message has to be assigned with a unique number and provided in the field Transaction Identification <TxId>. The UTR is unique for a transaction and is 22 characters in length, which can be used for further reference. The structure of UTR is “XXXXRCYYYYMMDDnnnnnnnn” where **XXXX** is IFSC (first 4 character) of sending member, **R** represents RTGS, **C** represents channel of the transaction, **YYYYMMDD** represents year, month and date of the transaction, **nnnnnnnn** denotes the sequence number. The list of channel codes is at [Annex 2](#).

6.3 *Message Standard*: RTGS shall handle messages based on ISO 20022 standard. Every payment message is validated for the mandatory fields and all the mandatory fields are validated in accordance with the ISO 20022 message standards and the coding requirements set by the Bank. If the message contains error code, it is returned to the originating member in the manner prescribed by the Bank. A list of error code is at [Annex 3](#).

6.4 *Transaction Type Code (TTC)*: RTGS uses a Transaction Type Code (TTC) to identify the type of individual payment messages that is allowed for the particular type of payment transaction. The TTC values are in the range of “0000” to “9999”. The list of active TTCs is given at [Annex 4](#). Members can also check the list online with the web front-end of RTGS application. TTC value shall be part of the message content. Members should use appropriate TTC Value while originating RTGS

transactions. The Bank shall have the right to change the list of TTC values from time to time.

6.5 Priority: The members may assign a priority while processing a payment transaction at the Member Interface before releasing the transaction to the Central System. The available range of priority is from '01' to '99'. The lower the number assigned, the higher shall be the priority. Priorities numbers "01" to "10" are reserved for the Bank and members can use priorities from "11" to "99". The transactions of the Bank are assigned with the highest priority followed by the MNSB and inter-bank transaction files. The Bank may change the priority number allocation as and when considered necessary with a due notification to the members. In case a participant other than the Bank enters priority numbers from 0 to 10, then RTGS shall assign a default priority number to the transaction and settle the same.

6.6 Queuing: Payment messages received in RTGS shall be maintained in a logical payment queue, pending settlement. The queue shall be ordered by priority numbers of the transactions and, within a priority number, by the time of receipt in RTGS. Transaction shall be taken up for settlement which is at the top of the payment queue. Members may cancel or re-prioritise transactions that are awaiting settlement in the payment queue.

6.7 Settlement: A payment transaction is determined and settled when the Settlement Account maintained with RBI of sending participant is debited and receiving participant is credited. On settlement, the payment transaction shall be treated as final and irrevocable.

6.8 Debit notification and Credit message: On successful settlement of any payment transaction the sending participant receives a notification and receiving participant receives the full payment message. The members accessing RTGS through the Thick Client/MI channel may put in place necessary interfaces with their host systems using Straight Through Processing (STP). The members accessing RTGS through Web and PO module should monitor their transactions (both debit and credit) on a continuous basis.

6.9 Duplicate Handling: Members have to choose the Copy Duplicate field tag in the Business Header of the payment message and fill relevant mandatory fields for handling duplicate transactions. If Copy Duplicate field tag is selected, the Central

System shall check whether the transaction has already been processed or not. Accordingly, the transaction shall be processed by the Central System.

6.10 *Positive confirmation:* A message format (camt.059) is available to communicate an acknowledgement to the remitting bank containing the date and time of credit to beneficiary account. This message would flow from the beneficiary bank to the remitter bank through SFMS. This feature is currently available for member banks wherein both remitter and beneficiary banks access RTGS through Thick Client / MI channel. The feature would be subsequently extended to members accessing RTGS through other channels as well.

Chapter – 7

RTGS Business Day and Operating Sessions

7.1 RTGS shall operate on all days. Any changes to the operating calendar or any declaration of holidays shall be communicated to the members by means of a broadcast message and / or publication on the Bank's website.

7.2 RTGS shall operate round the clock on all days of the year with the business hours for posting transactions decided by the Bank in consultation with the stakeholders. However, the Bank may, at its discretion, change the operating hours of RTGS for a particular day or for any period with prior notification.

7.3 RTGS daily events

7.3.1 *Start of Day (SOD)*: This is the first event which triggers basic functions of the system viz., advancing of system's business date; loading the updated code files; and accepting payment instructions from the internal systems of the Bank. Payments sent by the members are not accepted for settlement at the time of SOD. If submitted, payments are kept in queues, waiting for the next event to be executed. To transfer opening balances to settlement account from the member's current account maintained in e-Kuber system (SOD balance transfer), a member has to provide necessary undertakings to the Regional Director, Reserve Bank of India, Mumbai Regional Office, Main Building, Fort, Mumbai 400 001. The SOD balance transfer of existing RTGS members shall be continued in RTGS as per the undertakings already submitted for this purpose.

7.3.2 *Open for Business (OFB)*: This event marks the moment when all the functionality of RTGS is fully available to the participants. The system starts processing all types of messages. Intra-day liquidity (IDL) facility shall be available to the eligible participants after Open for Business operation in RTGS. The details of IDL facility is covered in the Section 8.

7.3.3 *Cut-off*: The cut-off represents the end of all business operations conducted by a member for the business day. All transactions i.e. customer transactions, interbank transactions, return transactions etc. except the MNSB must be

submitted to RTGS before the cut-off. The Intra Day Liquidity (IDL) position of the participant must be reversed before this point. All pending transactions shall be automatically cancelled by RTGS and members transmitting funds shall be notified accordingly. MNSBs, however, can be submitted and processed after cut-off also, till EOD.

7.3.4 End of Day (EOD): This is the last event of a business day. There shall either be a positive or a zero balance in the settlement accounts. The balances of settlement accounts shall be swept back to the current accounts of respective banks maintained in e-Kuber.

7.3.5 MNSB files and MNSB Return files are permitted to be posted from the moment of Open for Business and before End of Day of RTGS. The Bank may, at its discretion, prescribe specific time windows for posting MNSB settlements of ancillary payment systems.

7.3.6 The Bank may, permanently or temporarily, change the timings of various business phases during the day at its discretion. The change in the hours shall be notified by the Bank to the participants through a broadcast message or publication on the Bank's website or both as decided by the Bank.

7.3.7 The time windows cannot be re-opened in RTGS once the cut-off is over.

7.3.8 The cut-off timings of RTGS have been stated in [Annex 5](#). The Bank reserves the right to change any operating session (either extend or shorten / compress the operating session). The Bank shall not be liable for any consequences, arising out of such change of the operating session.

7.4 Gridlock Resolution Mechanism: The system provides a gridlock resolution mechanism that resolves (to the extent possible) all outstanding queued transactions. This resolution process is automated and runs at a predefined time interval for the urgent stream of payments in the queue. The Bank is, however, in no way, obligated to settle queued transactions through this mechanism and no member of RTGS can claim any right to have its payment transactions settled through the gridlock resolution mechanism.

Chapter – 8

Intraday Liquidity (IDL) Facility

8.1 The Bank may, at its discretion, grant access to intra-day liquidity (IDL) facility to the members for the settlement of their payment transactions in RTGS to overcome short-term requirements for funds (during RTGS business day) for settlement of the transactions. The terms and conditions, under which such IDL shall be granted, may be amended from time to time. The decision of the Bank in this regard shall be final.

8.2 The Bank shall decide the eligibility criteria for IDL facility. RTGS members, eligible for IDL facility, shall enter into an IDL Agreement with the Regional Director, Reserve Bank of India, Mumbai Regional Office, in the prescribed format at the time of admission as a member. IDL is a repo facility and all terms and conditions of repo transactions shall accordingly be applicable. IDL shall be provided to eligible members against eligible collaterals, as decided by the Bank from time to time.

8.3 The quantum of IDL, margin requirement and nature of collaterals shall be notified by the Bank from time to time. The collaterals against which IDL facility is provided are Government of India dated securities and treasury bills maintained in IDL-SGL account.

8.4 IDL facility shall be invoked automatically for eligible members as and when they do not have the required funds in their settlement account for settling transactions. IDL shall be invoked in multiples of an amount decided by the Bank, subject to a maximum amounting to the securities earmarked in IDL-SGL account. Requests for IDL shall be sent to the Bank's e-Kuber for eligible collateral. If eligible collaterals are not available then e-Kuber shall decline the IDL requests. Further, requests for IDL shall be sent to e-Kuber at periodic intervals. However, members should ensure availability of eligible collaterals and the lien for IDL facility with the Bank to avoid repeated requests against the same IDL request. If such instances are observed, the Bank shall view it seriously and may impose penalties at its discretion. IDL shall be reversed automatically as and when the required funds are available in the settlement account of the members. The Bank has a right to introduce an upper limit for the number of IDL requests a member can make.

8.5 IDL funds shall be used by RTGS for the settlement of any transaction and not just for the transaction for which the IDL was requested.

8.6 IDL facility availed by a participant shall be automatically reversed by RTGS on availability of sufficient funds in the settlement account of the participant above a threshold level. The threshold level shall be set by the Bank at its discretion. The reversal of IDL shall be treated as a high priority transaction. IDL that is outstanding on account of insufficient funds in the settlement account is required to be repaid / reversed fully by the participant before RTGS cut-off is executed. If a RTGS member fails to repay any IDL availed by it before the Cut-off is executed, the same shall be reversed using the Current Account balance of the member. In case the IDL availed and pending reversal post execution of cut-off is greater than the Current Account balance of the member, the securities (excess of Current Account balance) against which such IDL was availed of and not repaid shall get transferred to the Investment Account of the Bank. In such a case, the participant shall be liable to pay the Bank, interest at twice the Repo Rate prevailing on the particular day.

8.7 On the following business day, the member shall repurchase the securities by 10 AM, failing which the member shall not have access to IDL facility till the repurchase is completed. If the member does not repurchase the securities within the stipulated period of time, the matter shall be viewed seriously by the Bank and the member may be liable for suspension from RTGS membership, in addition to imposition of additional penalties, as may be decided by the Bank.

8.8 The Bank may levy charges to a member for using IDL facility. The Bank may also, at its discretion, change the manner in which IDL is charged. The Bank reserves the right to withdraw the IDL facility at any point of time and the decision of the Bank in this regard shall be final.

Chapter – 9

Other Features of RTGS

9.1 *Hybrid feature*: RTGS has the facility of settling transactions on a Gross and off-setting (bilateral or multilateral offsetting) basis through its hybrid settlement features. The transactions shall be settled on a gross basis or liquidity optimization basis depending on priority of the messages in the relevant field tag. The Hybrid feature has been configured to do off-setting every 5 minutes. The transactions with normal priority would be settled in off-setting mechanism, with a maximum of two attempts i.e. the maximum time a transaction would be in “normal” queue is 10 minutes. If the transactions with normal priority are unable to be settled in offsetting mode within this time, the priority of the transaction would be automatically changed to “urgent”. The parameter value has been set to 10%. This means that 10% of the balance in the settlement A/c would be taken for settlement in the offsetting mode. The Bank may, at its discretion, make changes to this mechanism after due notification to the members.

9.2 *Setting bilateral and multilateral limit*: The Bank may set bilateral and multilateral counter party limits at the request of the members to discourage free riding on liquidity in RTGS. The Bank has the right to implement this after due notification to the members, subject to change from time to time.

9.3 *Future value dated transactions*: RTGS shall not accept future value dated transactions from the participants for settlement on future RTGS working days. However, the Bank has the right to implement this facility in future after due notification to members.

9.4 *Centralised Anti Money Laundering Filtering*: RTGS shall validate payment transactions with the negative list databases for AML / CFT as per the guidelines issued by the Bank. The Bank has the right to implement this after due notification to the members.

9.5 *Multicurrency*: RTGS shall process multicurrency transactions as per the guidelines issued by the Bank from time to time. The Bank has the right to implement this after due notification to the members.

Chapter – 10

Rights of Members / Participants

10.1 Participants / members are eligible to send / receive transactions to / from the central system during the business hours as approved by the Bank.

10.2 Participants / members have right to contact RTGS Helpdesk set up by the Bank for necessary assistance for RTGS operations.

10.3 Participants / members have right to make complaints / give feedback to the Bank on technical / business issues with regard to RTGS. Such issues may be brought to the notice of the Bank for further discussion in the Standing Committee.

10.4 Participants / members have right to make representations to the Bank on any issues related to RTGS.

Chapter – 11

Customer Transactions – Obligations and Rights of Members / Participants

11.1 Eligible members can send / receive customer transactions on behalf of their customers. The transaction originating member shall carry out due diligence while sending the payment request to RTGS. The originating member should ensure two factor authentications by adopting a maker-checker principle while originating a payment transaction. Depending on the risk perception, participants may introduce / implement additional security features in the on-line delivery channels for initiating RTGS transactions by the customers. The originating member should release the payment message from their system to RTGS central system within 30 minutes of debiting a customer's account. The originating member should have the facility of time stamping of their transactions at various stages for effective grievance redressal mechanism.

11.2 Credit under customer transactions, received by RTGS member in its Settlement Account through RTGS, shall be ultimately credited to the account of the beneficiary on the basis of the account number in the payment message. The payment message receiving member may put in place a Straight Through Processing (STP) mechanism for crediting the beneficiary's account. The beneficiary / receiving bank shall credit the account of beneficiary customer immediately on receipt of the payment message at their Member Interface. The beneficiary banks should credit the account of the beneficiary within 30 minutes of the receipt of the message at the Member Interface.

11.3 The members accessing RTGS through Web or PO module are required to continuously monitor their incoming transactions in the central system for adhering to the timelines prescribed by the Bank.

11.4 In case of any delay in providing credit to the beneficiary's account, the recipient / beneficiary's bank has to pay compensation at current repo rate plus 2% to the beneficiary customer for each day of delay. In case of delay in credit on the same day, a compensation for a day shall be paid to the customer. The

compensation amount should be credited to the customer's account automatically without any request.

11.5 In case, it is not possible to credit the funds to the beneficiary's account for any reason e.g. account does not exist, account frozen, etc., funds shall be returned to the originating member within one hour of receipt of the payment at the Member Interface of the recipient member, subject to availability of RTGS. The return payment shall be sent by the recipient bank in the prescribed message format stated in Chapter 5. The Unique Transaction Reference (UTR) / Transaction Identification Number should be same as that of the original message.

11.6 In case of any delay in returning the payment to the originating member, the recipient member shall be liable to pay compensation at current repo rate plus 2% to the originating member and the same shall be ultimately credited to the account of originating customer.

11.7 Customer transactions that are not settled in RTGS because of insufficient funds shall be viewed seriously. Recurrence of such incidents shall attract penal provisions as decided by the Bank.

11.8 All members should provide necessary information in the customer's account statement pertaining to their RTGS transactions as per the instructions issued by the Bank. In addition, members shall also provide information in the form of alerts or confirmations to customers, as stipulated by the Bank. Members are also required to provide a positive confirmation to the remitter on successful funds transfer to beneficiary. (This is mandatory in case of transactions where both remitter and beneficiary bank are accessing RTGS through the Thick Client / MI channels.)

11.9 Members can levy service charges for RTGS transaction to their customers as per the instructions issued by the Bank from time to time.

11.10 Members shall comply with the rules and regulations of FEMA and Wire Transfer Guidelines issued by the Bank from time to time. The sending participant shall provide account type "NRE" or "NRO" as applicable in the Debtor's (Sender's) Account Type wherever required.

11.11 Members shall mandatorily provide Debtor Name (the ordering customer) and Creditor Name (the beneficiary customer). The member banks shall furnish name of the beneficiary in the passbook / account statement of originator and name of

ordering customer in the passbook / account statement of beneficiary from these field tags.

11.12 Members shall provide necessary description in the passbook / account statement of their customer for RTGS return transactions. The originating bank shall populate necessary information from the ISO message and provide the same to the customer. The originating participant shall provide the description “RTGS-RETURN-<Original UTR Number>-<Intended Beneficiary Customer>-<Reason for Return>”.

11.13 The Bank has the right to issue additional instructions to members for customer transactions from time to time.

11.14 The Bank may introduce or remove threshold value for any transactions type in RTGS, in future, with due notification to the members. The existing floor limit for customer transactions is at [Annex 6](#).

11.15 Members should put in place necessary infrastructure to provide RTGS round the clock to their customers. RTGS transactions undertaken after normal banking hours are expected to be automated using ‘Straight Through Processing (STP)’ modes.

Chapter – 12

MNSB Settlement and Clearing House Participants

12.1 As stated in the chapter 4, Clearing entities shall be permitted to submit Multilateral Net Settlement Batch (MNSB) files emanating from the ancillary payment systems managed by the Clearing entity.

12.2 The Clearing entities that have been granted membership or limited access to RTGS shall abide by the terms and conditions stipulated in the access criteria and / or any other additional / specific conditions stipulated by the Bank from time to time.

12.3 The Clearing entities shall ensure that all their clearing members have current accounts and settlement accounts or both with the Bank. The Bank has the right to settle the MNSB files in the e-Kuber which are normally posted in RTGS, and vice versa, in case of any eventuality or as a BCP measure.

12.4 The Bank may, at its discretion, specify a particular time window for posting the MNSB files in RTGS for settlement.

12.5 The Clearing entities shall ensure that their clearing members maintain adequate funds in the settlement account or the current account maintained with the Bank.

12.6 The MNSB file submitted by a Clearing entity would settle in RTGS on an all or none basis. In case of insufficient funds in one or more clearing member's settlement account, the entire MNSB file shall be pending for settlement. The system shall retry at periodic intervals for a certain number of times (as decided by the Bank from time to time) to reassess the funds position in the concerned member/s' settlement account/s. If the MNSB file remains pending, the sponsorship arrangement / lines of credit arrangement of the Clearing entity shall be invoked, if available, for funding the required shortfall. In case, funds are insufficient for the settlement of the MNSB file, then the MNSB file shall be returned to the Clearing House concerned.

12.7 Any delay in the settlement of an MNSB transaction, due to failure on the part of member/s to ensure availability of adequate liquidity to meet their respective debit obligations, shall be viewed seriously by the Bank. Penalty may be levied at the

discretion of the Bank if continued instances of shortfall in funds for MNSB settlement are observed for any member. The Bank is not responsible for any delay in settlement or return of the MNSB file to the Clearing entity due to short of funds in the current / settlement accounts of their clearing members.

12.8 The Bank may instruct the Clearing entity for opening of limited purpose settlement account in RTGS by their clearing members having current account with the Bank but are not a direct member of RTGS.

12.9 On successful settlement of MNSB file, the debit and credit notifications shall be sent to the members of the clearing entity. RTGS shall send notifications to the members of the clearing house for debits / credits in the settlement account.

12.10 The Clearing entity, which submitted the MNSB transaction for settlement, affected by an MNSB transaction, shall be notified by the Central System on settlement of the MNSB transaction. In case of an MNSB file is cancelled / rejected, the Clearing Entity shall be notified of the reason for failure, including details of the clearing participants, who failed to meet their debit obligations as well as the actual amount of shortfall.

12.11 No Clearing Entity shall be permitted to cancel an MNSB transaction, once it has been received by the Central Systems. An MNSB transaction can be cancelled by the Bank only.

Chapter – 13

Obligations and Duties of Members / Participants

13.1 All members / participants are required to closely monitor their liquidity positions. RTGS settlement accounts of members / participants are required to be funded adequately so that gross and MNSB transactions are settled smoothly. Queuing of transactions and delay of MNSB file settlement due to liquidity considerations shall attract penal action including suspension of membership.

13.2 Members shall implement necessary infrastructure for accessing the Central System at RBI on its Payment Gateway. The systems specifications should comply with the Bank's instructions / guidelines. Members should do regularly maintenance of the systems to avoid any failure of hardware, network and software and put in place the Business Continuity Plan as per the guidelines specified by the Bank from time to time.

13.3 In case of any failure of the system resulting in non-operation of the system at the member end, the member should report to the Bank at the earliest and not later than 30 minutes of the incidence. The members have to adhere to the Business Continuity Plan (BCP) / Disaster Recovery (DR) guidelines as notified by the Bank from time to time.

13.4 The Legal Entity Identifier (LEI) is a 20-digit number used to uniquely identify parties to financial transactions worldwide. The sending participant should include remitter and beneficiary LEI information in RTGS payment messages for all customer and interbank payment transactions of value ₹50 crore and above undertaken by entities (non-individual) . For transactions, where either or both parties are non-individual/s, LEI will be required. It is not necessary for Governments or their Departments / Ministries to obtain LEI or mention LEI number for payment transactions in RTGS. However, Corporations / Undertakings, including those fully owned by the Government, shall need to obtain LEI. Accordingly, all single payment transactions of ₹50 crore and above of Government Undertakings and Corporations, through RTGS, shall include remitter and beneficiary LEI information. Details of the identified fields in the messaging structures of RTGS for inclusion of LEI information

are given at [Annex 7](#). Any inward transaction with inappropriate or no LEI should not be rejected by beneficiary bank. Member banks should maintain records of all transactions of ₹50 crore and above through RTGS.

13.5 Under the FCRA, 2010 (amended as on September 28, 2020), foreign contribution must be received only in the “FCRA account” of State Bank of India (SBI), New Delhi Main Branch (NDMB). The contribution to the FCRA account are received directly from foreign banks through SWIFT and from Indian intermediary banks through RTGS systems. In terms of extant requirements of Ministry of Home Affairs (MHA), Government of India, the donor details such as name, address, country of origin, amount, currency, and purpose of remittance are required to be captured in such transactions and SBI is required to report the same to MHA on daily basis. Participants are advised to capture the requisite details while forwarding the foreign donations through RTGS systems to SBI as given in [Annex 8](#). Member banks are advised to incorporate necessary changes in their core banking / middleware solutions to capture the requisite details while forwarding the foreign donations through NEFT and RTGS systems to SBI.

13.6 Members shall adhere to the information security guidelines/advisories issued by the Bank from time to time.

13.7 Members shall furnish complete information of the payment transactions in the prescribed message format while originating transactions stipulated by the Bank from time to time.

13.8 Members shall not at any time assign, lease, license or dispose of to any other person, trust, company or corporation including its subsidiaries in whole or in part, RTGS services, including the software, provided by the Bank or any benefit or advantage derived therefrom.

13.9 Members shall comply with the circulars, notifications, instructions etc. issued by the Bank from time to time with regard to RTGS. Members shall also ensure continued adherence to regulatory framework for INFINET.

13.10 Members are required to provide such information as may be called for by the Bank in respect of RTGS.

13.11 The Bank may, at any time, conduct or get conducted audit and inspection of the member's site with or without any prior notice.

13.12 Members shall pay service charges / membership fees / transaction fees, if any, as notified by the Bank. The member is liable to pay monthly membership fees irrespective of the number of days a member was active in a particular month. The Bank has the right to debit such service charges / membership fees / transaction fees from the member's current account / settlement account maintained with the Bank. The Bank may, at its discretion, levy tariffs on various system events associated with the transactions. These charges are subject to revision from time to time. The Bank may, if required, levy any other additional charges⁴. The present service charges for participants / members are at [Annex 9](#). The Bank has waived the transaction fees in RTGS with effect from July 01, 2019.

13.13 Members should maintain RTGS transactions data for at least 10 years or such time period as specified by the Bank from time to time. For members using the PO module, the data shall be available in RTGS.

13.14 The Bank may suspend / terminate the membership if the participant is suspended from any other associated system(s) like SFMS, INFINET etc.

13.15 The Bank has the right to suspend / terminate the membership in case of non-compliance of any instructions issued from time to time. The Bank shall have the authority to determine if a member can continue to participate in RTGS, or not. The Bank shall have the right to suspend or terminate the membership, if continuation of the member is viewed to be detrimental to the smooth functioning of RTGS in any manner.

13.16 A member shall continue to be liable and responsible for the contents of the messages sent by it, even if it subsequently it resigns or is suspended or its membership is terminated.

13.17 A member shall be directly and wholly liable in respect of all its customers and with reference to all the transactions, executed on RTGS on behalf of such customers and the Bank shall in no way be responsible either for the source or usage of funds involved in the transactions.

⁴ The Bank has waived the processing charges and time varying charges levied on banks for outward transactions undertaken using the RTGS System with effect from July 1, 2019.

Chapter – 14

Sub-Membership in RTGS

14.1 Direct members can extend RTGS facility to licenced banks which have the technological capabilities but are not participating in RTGS on account of either not meeting the access criteria or because of cost considerations. The direct member is a sponsor bank and the licensed bank accessing RTGS through a sponsor bank is a sub-member. Non-bank PSPs cannot act as sponsor member or participate as a sub-member in the RTGS (or NEFT).

14.2 The sponsor banks would be responsible for sending / receiving the transactions / messages on behalf of their sub-member(s).

14.3 The obligations and duties in respect of customer transactions viz., timely credit and return are applicable to the sub-members also.

14.4 There are no restrictions on the number of sub-members a sponsor bank can sponsor. Aspects relating to operational feasibility, risk mitigation, fund settlement, collaterals etc., are the responsibility of sponsor bank.

14.5 The sponsor bank should put in place a risk management framework and a system of continuous monitoring of the risk management practices of sub-member(s) they sponsor. The risk management framework should be approved by the Board of the sponsor bank.

14.6 The settlement of transactions by / on the sub-members would take place in the settlement accounts of the sponsor banks maintained with the Bank. The sponsor bank under this arrangement shall assume complete responsibility for the settlement of all transactions pertaining to their sub-members.

14.7 The sponsor bank at all times should ensure that its sub-member/s adhere to and abide by the rules, regulations, operational requirements, instructions, orders, decisions etc., of RTGS, as laid down by the Reserve Bank from time to time.

14.8 Redressal of all customer complaints / grievance would be the responsibility of the sponsor bank. To aid in this process, the sponsor bank should ensure that the sub-member/s have put in place a transparent and robust mechanism to resolve

customer complaints in a quick and efficient manner, as laid down in the procedural guidelines, business rules and regulations of RTGS.

14.9 All disputes between the sponsor bank and the sub-member/s shall be handled bi-laterally amongst them.

14.10 The sponsor bank shall bring to the immediate notice of the Bank:

- (i) any involvement of its sub-member/s in any suspicious transactions, frauds, etc.;
- (ii) any of its sub-member/s resorting to unfair practices relating to their participation in RTGS;
- (iii) any of its sub-member/s not adhering to the rules, regulations, operational requirements, instructions etc., of RTGS;

14.11 The sponsor bank is not required to take prior approval of the Bank for sponsoring sub-member/s to RTGS. However, as and when a sponsor bank admits a sub-member, the sponsor bank is required to immediately inform the Regional Director, Reserve Bank of India, Department of Payment & Settlement Systems, Mumbai Regional Office, Mumbai, regarding the details of the sub-member/s, IFSC allotted to the branch / branches of the sub-member/s, date of commencement of sub-membership etc. Further, every direct member bank shall submit to the Bank a list of its sub-members, as on March 31 every year. The list is to be submitted to The Regional Director, Reserve Bank of India, Department of Payment & Settlement Systems, Mumbai Regional Office.

14.12 The sponsor bank should immediately inform the Bank the cessation of sponsorship arrangement between the sponsor bank and sub-member/s.

14.13 The charges for customer transactions of sub-member/s cannot exceed the maximum charges prescribed by the Bank from time to time.

14.14 A sub-member shall directly report any fraud in Central Payments Fraud Information Registry (CPFIR).

Chapter – 15

Dispute Resolution and Miscellaneous

15.1 The Bank shall endeavour to ensure proper operation, control, maintenance and security of RTGS. The Bank shall not be responsible for the loss, if any, that may be caused to members or their customers or any person, arising out of any action taken in good faith by the Bank's staff or malfunctioning or break down of the computer systems, computer network, telecommunication network or any other equipment (inclusive of hardware and software), used in RTGS or any force majeure conditions.

15.2 The Bank shall issue necessary guidelines on Dispute Resolution Mechanism from time to time. The disputes between two members of RTGS should be addressed to the Regional Director, Reserve Bank of India, Mumbai Regional Office, Main Building, Shahid Bhagat Singh Marg, Fort, Mumbai - 400001. In the event of any difference or dispute, arising between any two members in connection with RTGS or incidental thereto, the dispute shall be resolved by the Bank as per the guidelines issued on Dispute Resolution Mechanism by the Bank from time to time.

Customer Service / Facilitation

15.3 The members shall set up customer facilitation centre (CFCs) for handling complaints related to RTGS transactions. The details of customer facilitation centers viz., nodal person and contact numbers have to be displayed by the members on their website and at branches. These details have to be shared with the Regional Director, Reserve Bank of India, Mumbai Regional Office, Main Building, Shahid Bhagat Singh Marg, Fort, Mumbai- 400001.

15.4 The customers of members may send their complaints to the Chief General Manager, Reserve Bank of India, Customer Education and Protection Department, Amar Building, 1st Floor, Sir P. M. Road, Fort, Mumbai - 400 001.

15.5 The Bank has the right to levy penalties or any other punishment like suspension, termination etc. to the members in the event of violation of the guidelines, instructions etc. issued by the Bank from time to time.

15.6 The Bank has the right to frame additional guidelines / amendments to the existing guidelines as deemed fit from time to time.

Chapter – 16

Disclosures

16.1 The Bank, in the interest of banking or monetary policy or the operation of the payment systems generally, or in the public interest, may disclose such information as deem fit and proper to any person.

16.2 The member's transactions, including their customer transactions, settled or rejected through RTGS, may be shared, as deemed necessary by the Bank, with Regulatory Authorities, Government and other appropriate authorities.

Chapter 17

Cyber Security Guidelines for RTGS

17.1 All members of RTGS are expected to be in compliance with the base line cyber security guidelines provided at [Annex 10](#) at the time of going live and on an ongoing basis.

17.2 All members shall get conducted audit of their RTGS related systems by a CERT-In empanelled IS auditor once a year and submit the report to the Bank.

17.3 The auditors conducting audits, need to follow applicable IS audit standards to provide reasonable assurance to RBI about the status of compliance to baseline cyber security guidelines. The IS audit report shall be accompanied with the IS audit standards followed by the auditor along with detailed IS audit procedures employed. The report shall also be accompanied with artifacts and evidence collected in respect of each item to substantiate its observations.

17.4 The audit report and compliance certificate are to be submitted to Mumbai Regional Office, RBI in the manner and as per timelines specified from time to time. These reports will form the basis for deciding on the grant of membership as well as the continued participation of the existing member in RTGS.

17.5 Sponsor banks shall also specify minimum cyber security requirements for its sub-members and ensure that they are met.

17.6 Apart from these guidelines, all members shall comply with the applicable Cyber Security Framework, advisories and related regulatory requirements prescribed by RBI/ NABARD/ applicable regulatory body.

Annex 1

Transaction Type, Message Formats and Major Rules

Transaction Type	Message format and rules
<i>Inter-institutional / inter-bank transaction</i>	The ISO message format for this transaction type is “pacs.009.001.03 - FinancialInstitutionCreditTransferV03” with transaction type code as “1400” and priority from “12” to “99” in the sub-field tag Proprietary <Prtry> (TTC=1400, PRIO=35) of field tag Service Level <Svcvl>. The sub-field Proprietary <Prtry> of the field LocalInstrument <LclInstnm> have to be provided with “RTGSFIToFICredit”.
<i>Customer transaction</i>	The ISO message format for customer transaction is “pacs.008.001.03 FIToFICustomerCreditTransferV03”.
<i>Government transaction</i>	The ISO message format for Government transaction is same as inter-institutional / inter-bank transaction with purpose code “GOVT” in the sub-field tag Code <Cd> of field tag Category Purpose <CtgyPurp>. The necessary challan information is to be provided in the field tag RemittanceInformation <RmtInf>.
<i>Multilateral Net Settlement Batch (MNSB)</i>	The ISO message format for this transaction type is “pacs.009.001.03 - FinancialInstitutionCreditTransferV03” with transaction type code as “XXXX” and priority from “11” to “11” in the sub-field tag Proprietary <Prtry> (TTC=XXXX, PRI=11) of field tag Service Level <Svcvl>. The sub-field Proprietary <Prtry> of the field LocalInstrument <LclInstnm> have to be provided with “RTGSNetSettlementXXzNN”. Here XX stands for type of MNSB file, viz. GC-guaranteed settlement of Securities and CBLO segment; IB-guaranteed settlement of FOREX segment; FX-non-guaranteed settlement; MC-MICR Clearing; SE-non-guaranteed MNSB; OT-other MNSBs. Here ‘z’ in the indicator takes vales C-Original; R-Return and L-Last Return. NN is the return serial number.
<i>Delivery versus Payment (DvP)</i>	These transactions are generated by RTGS for availing intra-day liquidity (IDL) facility provided by the Bank. RTGS automatically sends request to the e-Kuber system of the Bank for IDL as and when the participants do not have required funds in their settlement account. ISO format is used for this transaction and message type is pacs.009.001.03
<i>Own Account Transfer (OAT)</i>	The ISO message format for this transaction type is “pacs.009.001.03 - FinancialInstitutionCreditTransferV03” with transaction type code as “1800” and priority from “12” to “99” in the sub-field tag Proprietary <Prtry> (TTC=1800, PRI=35) of field tag Service Level <Svcvl>. The sub-field Proprietary <Prtry> of the field LocalInstrument <LclInstnm> have to be provided with “RTGSOwnAccTransfer”.
<i>Return Payment Transaction</i>	The ISO message format for this transaction type is “pacs.004.001.03 PaymentReturnV03” with the reasons of return to be mentioned in Reason <Rsn> Code <Cd>.

Annex 2**Channel Codes for UTR / Transaction Identification**

Channel ID	Values
RTGS	9
Internet Banking	1
Cash Management	2
Treasury	3
ATM	4
Other	5

Annex 3

Codes on Message Validation in RTGS

Code	Internal RTGS Code	Description
001	INVDATEFMT	The received message had an invalid date
002	INVCREDINST	Invalid credit institution
003	INVDEBINST	Invalid debit institution
004	INVSND	Invalid message sender
005	INVRCV	Invalid message receiver
007	INVPART	The participant is invalid
008	INVCURR	The received message specifies an invalid currency.
009	INVAMT	The amount is invalid
010	DUPREF	Duplicate reference
011	INVDATE	The received message has an invalid date: past date.
012	INVDATEEOD	The message specifies a date which is closed already for business.
013	INVDATEIC	The message was received after Initial Cutoff.
014	INVDATEFC	The message was received after Final Cutoff or invalid IDL window state.
015	INVBUSSDATE	The received message refers a not working business date.
016	INVBUSSDATEFUTURE	The value date is ahead with more than the allowed number of days.
017	INVMTTYPE	The received message has an invalid (unsupported) message type.
018	INVSIG	The digital signature could not be verified (failed the validation)
020	INVDEFPROCTTC	No default TTC defined for this type of transaction.
021	INVTRANTYPEFORTTC	The TTC specified belongs to a different Class of TTCs and cannot be used (transaction type and TTC do not match).
022	INVTTCPARTTYPE	The TTC cannot be used with this sender's Participant Type.
023	INVRESERVEOWNER	The owner of the requested reserve operation does not match the sender.
024	CANUSR	Transaction was cancelled manually in RTGS by an RTGS user.
026	CANPENTIME	Transaction was cancelled due to exceeded amount of time it was in Pending
027	CANFCO	Transaction cancelled automatically by RTGS at Final Cutoff

Code	Internal RTGS Code	Description
028	CANINVDEB	Invalid debtor in MNSB part (account or participant cannot be found); Debit party is not RBI in case of IDL
029	CANINVCRED	Invalid creditor in MNSB part (account or participant cannot be found)
098	INVFMT	An invalid message was received which cannot be validated against the XML schema.
099	INVFMT	An invalid message was received which didn't pass at least one schema rule validation.
040	INVCREDAGENT	An invalid credit agent value was found in the message
041	INVDEBAGENT	An invalid debit agent value was found in the message
038	INVDOUBLEReturn	A second return instruction was received for the same original instruction

Annex 4

List of TTC Values and Priority for RTGS

TTC Value	Transaction Type	Priority Range	Default Priority	IDL Facility	Members Eligible
1000	Customer	12-99	35	Yes	A
1400	Inter-bank	12-99	35	Yes	A, B
1800	Own Account	12-99	35	No	A, B, D
3000	MNSB	11-11	11	Yes (for members)	C, D
3200	Inter-bank	12-99	35	No	D
3500	Customer	0-10	5	No	RBI
3600	Inter-bank	0-10	5	No	RBI
3700	MNSB	0-10	5	Yes (for members)	RBI
4000	Customer	12-99	45	No	D
3100	Mixed MNSB	11-11	11	Yes (for members)	C,D

Annex 5

Cut-off Timings in RTGS at RBI (effective December 14, 2020)

Time event of RTGS is as follows:

Sr. No.	Timing / Event	All days
1.	Open for Business	00:30 hours
2.	*Cut-off (Customer and Inter-bank transactions)	23:50 hours
3.	#End of Day	00:00

**The cut-off for customer (erstwhile initial cut-off) and interbank transactions shall be executed at 23:50 hours in RTGS.*

#RTGS End of day shall be undertaken after the cut-off has been executed and any IDL availed during the day has been reversed. This is undertaken in sync with the e-Kuber End of Day.

Annex 6

RTGS Threshold Value and Maximum Service Charges for Customers**Table 1: RTGS Threshold**

S. No.	Transaction Type	Threshold Value
1.	Customer	Rs. 2 lakh (floor limit)

Table 2: Maximum Service Charges Members Can Levy to the Customers

S. No.	RTGS Transaction Type and Value Band	Maximum customer charges
1.	Inward transactions	Free
2.	Outward transactions	
2a.	₹ 2 lakh to ₹ 5 lakh	₹ 25/-
2b.	Above ₹ 5 lakh	₹ 50/-

Annex 7**Capturing Legal Entity Identifier in RTGS Message**

In RTGS customer payment and inter-bank messages, the optional field “<-RmtInf->” has 4 repeat tags with each having 140 characters. The first two loops of this field shall be used for capturing sender and beneficiary customer LEI information, in that order, where applicable and available. When LEI information is captured, narration, remarks, etc., shall be part of last two repeating loops of the field. The sender and beneficiary information shall be captured in following format:

<-RmtInf-> loop 1 -> /SL/20 digit sender LEI/
loop 2 -> /BL/20 digit beneficiary LEI/

The LEI instructions are applicable to all the channels being used for connecting to RTGS viz. thick-client, Web-API (through INFINET or any other approved network) and Payment Originator (PO) module.

Annex 8

FCRA related transaction code in RTGS System

A) FCRA Transaction Code in RTGS System:

Originating banks are required to select the following mandatory fields of RTGS system while remitting foreign donations to the FCRA account at SBI:

Field	Type	Code to be used
PmtTplnf/CtgyPurp/Cd (in Pacs.008 message)	RTGS	FCRA

B) Format for providing Donor Details in 7495 and Rmtlnf fields of NEFT and RTGS System:

Originating banks are required to pass on donor details in the following formats in 'Rmtlnf' tag of RTGS:

System	Field / Tag	Code to be used	Transaction without Legal Entity Identifier (LEI) details	Transaction with LEI details
RTGS	PmtTplnf / CtgyPurp / Cd (in Pacs.008 message)	FCRA	Tag- Rmtlnf/Ustrd loop 1: Name of the donor loop 2: Donor Address loop 3: Purpose of the Remittance- Alphanumeric loop 4: Country of the Donor, currency, and Amount Alphanumeric	Tag- Rmtlnf/Ustrd loop 1: /SL/20-digit sender LEI/ loop 2: /BL/20-digit beneficiary LEI/ loop 3: Purpose of the Remittance – Alphanumeric loop 4: Country of the Donor, currency, and Amount - Alphanumeric

Annex 9**RTGS Service Charges for Members**

RTGS service charges has three components viz., (a) monthly membership fee, (b) transaction fee and (c) time-varying tariff for members and are as follows (effective June 1, 2019) –

(a) Membership fees

Type of Entities	Monthly Membership Fee (exclusive of taxes, if any)
Scheduled Commercial Banks (SCB)	₹ 5,000
Banks other than SCBs, Primary Dealers, clearing entities, other special entities, etc.	₹ 2,500

(b) Transaction fee (per transaction): The transaction fee has been waived with effect from July 01, 2019.

(c) Time varying tariff: The time-varying charges have been waived with effect from July 1, 2019.

The members shall pass on the above benefits to their customers for undertaking transactions using the RTGS system.

Annex 10**Baseline Cyber Security Guidelines for RTGS**

1. Inventory Management:
 - Maintain an up-to-date inventory register of all information assets.
 - Not to use outdated and unsupported hardware or software and monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.
2. Prevent installation of unauthorized software: Put in place a mechanism to control installation of software/ applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. In addition, put in place a mechanism to block/ prevent and identify installation and running of unauthorised software/ applications on such devices/ systems.
3. Network Security:
 - Use firewalls to protect the network perimeter
 - Ensure perimeter security and block all unnecessary ports
 - Ensure network segmentation to restrict lateral movement of attackers
 - Disable Remote Desktop Protocol (RDP). Restricted access in case of exceptions, may be provided only on need basis through Multi Factor Authentication and with appropriate monitoring.
 - Internet usage is strictly prohibited in SFMS/NEFT/RTGS infrastructure including the zone where these infrastructures are hosted.
4. Change and Patch Management: Ensure robust and documented change management process to assess, approve, implement and review changes made to any technology stack items associated with RTGS systems. Put in place systems and processes to identify, track, manage and monitor the status of patches to all concerned systems (servers, desktops, network devices, operating system and application software).

5. Access Management:
 - Implement strict user access controls based on principle of least privilege.
 - Implement multi-factor authentication (MFA) for all critical applications, especially for privileged accounts.
6. Email Security: Implement secure mail and messaging systems that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc. Implement DMARC (Domain based Message Authentication, Reporting & Conformance).
7. Continuous surveillance: Implement mechanism to detect and remedy any unusual activities in critical systems, servers, databases, network devices and endpoints.
8. Disaster recovery drills for critical systems should be conducted at least once in a half-year, preferably once a quarter.
9. Backup: Maintain regular and secure backup of critical data and systems, with tested recovery procedures in place.
10. If the entity is providing digital payment products and services to its customers, then ensure compliance to Master Direction on Digital Payment Security Controls related to Internet/ Mobile Banking (refer RBI Circular DoS.CO.CSITE.SEC. No.1852/ 31.01.015/ 2020-21 dated February 18, 2021), as updated from time to time.
11. Application Security Life Cycle (ASLC): Follow a 'secure by design' approach in the development of critical applications. Further, ensure that applications are inherently more secure by embedding security within their development lifecycle.
12. Log management: Put in place comprehensive log management procedures addressing aspects of identification of log sources, log generation, log transmission and storage, log normalisation & parsing, log analysis, log disposal, log security and periodic review of log readiness.

13. Conduct Vulnerability Assessment (VA) and Penetration Testing (PT): For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA to be conducted at least once in every six months and PT at least once in 12 months. The risks highlighted to be remediated within defined timelines based on criticality.
14. Cryptographic Controls: The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. Internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable should be adopted, and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.
15. Members to follow the latest IDRBT CA guidelines related to cryptographic devices and digital certificates. Entities should maintain and operationalize required policy in order to ensure that renewal of Digital Security Certificates (DSCs) are undertaken before expiry of ongoing certificates.
16. Transaction Monitoring: Implement mechanism for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.
17. Security Operations Centre(SOC): Set up SOC as provided in Annex-2 of Circular DBS.CO/CSITE/BC 11/33.01.001/2015-16 dated June 02, 2016 on Cyber Security Framework in Banks, as applicable and also factor in DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 on Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach , as applicable.
18. Adherence to rules & guidelines of INFINET, INFINET framework and SFMS, as updated from time to time.

Annex 11

Application Form for Approval for Membership of Centralised Payment Systems

<On the letter head of the applicant>

The Chief General Manager
Department of Payment & Settlement Systems
Reserve Bank of India
Central Office
14th Floor, Central Office Building
Shaheed Bhagat Singh Marg
Mumbai- 400 001

Dear Sir/Madam,

Approval for Membership of Centralised Payment Systems

We hereby submit an application in terms of RTGS System Regulations, 2013 for the following: (please tick as applicable)

- a. Membership to RTGS
- b. Membership to NEFT
- c. Current account with Banking Department, RBI,Regional Office
- d. SGL & IDL-SGL account with RBI
- e. NDS-OM & NDS-CALL membership with RBI
- f. INFINET membership

2. We declare that the information furnished are true/current and complete to the best of our knowledge and belief.

Yours faithfully

Signature:
Name:
Designation:
Company Seal:

Date:
Place:

Encls:

Part-A: General Information

1	Name of the applicant:	
2	Constitution of the applicant: Bank/Financial Institution/standalone Primary Dealer/ other entity	
3	Statute under which the applicant is incorporated/established:	
4	Status (For banks only): a. Licensed/Unlicensed: b. Scheduled/Non-scheduled:	
5	Registered Office Address:	
6	Date of incorporation:	
7	Date of commencement of business:	
8	Name of the concerned Regulatory/Supervisory Department of RBI or other regulator Insurance Regulatory and Development Authority (IRDA) / Securities and Exchange Board of India (SEBI), etc., as the case may be:	

9	Payment system/s for which membership/s is/are desired: a. Real Time Gross Settlement System (RTGS) b. National Electronic Fund Transfer System (NEFT)	
10	Type of RTGS membership sought (Regular/Restricted/Clearing House):	
11	Total number of branches/offices of the entity and number of branches likely to participate in the RTGS and NEFT respectively:	
12	Expected transaction volume/value (for RTGS and NEFT respectively):	
13	Payment system/s in which the applicant is currently participating: (if sub member, details of sponsorship should be given)	
14	Status of availability of Current Account with Banking Department, RBI: Yes/No If yes, details of the Current Account may be provided.	
15	Status of availability of SGL IDL-SGL with PDO Mumbai: Yes/No If yes, details of the SGL / IDL-SGL account may be provided.	
16	Whether entity is having NDS-OM membership: Yes/No If yes, details of the NDS-OM membership?	

17	Whether entity is having NDS-CALL membership: Yes/No If yes, details of the NDS-CALL membership?	
18	Whether the applicant is a member of INFINET: Yes/No If yes, certificate of INFINET membership may be provided.	
19	Details of earlier approval for RTGS/NEFT: Reasons for not completing participation may be informed.	
20	Details of nodal officer for RTGS/NEFT membership process:	

In case of insufficiency of the space for any point, information may be provided on a separate page on applicant's letter head.

Part - B: Financial and Risk Management aspects

1. Financial indicators:

Financial Parameter	As per last audited balance sheet
CRAR	
Net NPA	
Net Worth	
Net profit/loss in last two years	

Note: For entities for which the financial indicators are not available and/or applicable, they may indicate so.

Part - C: Additional documents

1. Purpose for applying for direct membership of centralized payment system (RTGS and NEFT)
2. Certificate of authorization/license/registration from the regulator
3. Certificate of Incorporation – certified true copy to be provided
4. Certificate of Commencement of business – certified true copy to be provided.
5. Audited Financial Statements for past two financial years
6. Auditor's certificate for Net worth and Net NPA (for banks) at the end of last financial year
7. Latest IS audit report of the entity including compliance to storage of payment system data instructions
8. Details of all the constituent accounts (specifying the number of gilt accounts maintained along with the name of the Primary Member)
9. Details of availability of Core Banking Solution / centralized processing system at applicant's end
10. Details of IT Infrastructure available and gap analysis
11. Risk management framework in place or being planned to be in place for participating in the payment systems
12. Risk management framework in place or being planned to be in place for operating SGL and/or CSG account
13. Copy of cancelled cheque