TO BE PUBLISHED IN THE GAZETTE OF INDIA, EXTRAORDINARY, PART III, SECTION 4

TELECOM REGULATORY AUTHORITY OF INDIA

**NOTIFICATION**

**New Delhi, the 19th July, 2018**

No. 311-04/2017-QoS: - In exercise of powers conferred by section 36 read with sub-clause (v) of clause (b) and clause (c) of sub-section (1) of section 11 of the Telecom Regulatory Authority of India Act 1997 (24 of 1997), the Telecom Regulatory Authority of India hereby makes the following regulations, namely:-

# THE TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCE REGULATIONS, 2018
(6 of 2018)

IndiaCode

## CHAPTER-I

## Preliminary

1. **Short title and commencement.** -

(1) These regulations may be called the Telecom Commercial Communications Customer Preference Regulations, 2018.

(2) (a) Except as otherwise provided in clause (b), (c), (d) and (e) these regulations shall come into force from the date of their publication in the Official Gazette;

(b) regulations 4,5,11,15,28,34, 35 and 36 of these regulations shall come into force after 30 days from the date of publication of these regulations in the Official Gazette;

(c) regulations 6, 13 and 14 of these regulations shall come into force after 90 days from the date of publication of these regulations in the Official Gazette;

(d) regulations 3, 7, 8, 9, 10, 12, 18 and 32 of these regulations shall come into force after 120 days from the date of publication of these regulations in the Official Gazette;

(e) regulations 23, 24, 25, 26, 27, 29 of these regulations shall come into force after 150 days from the date of publication of these regulations in the Official Gazette;

2. **Definitions**. - In these regulations, unless the context otherwise requires-

(a) **"Abandoned Call"** means an outgoing call in which the sender does not connect the call to a live agent after the call is established and is answered by the recipient.

(b) **"Access Providers"** includes the Basic Telephone Service Provider, Cellular Mobile Telephone Service Provider, Unified Access Service Provider, Universal Access Service Provider and Virtual Network Operator (VNO) as defined in the respective licenses issued by Department of

Telecommunications (DoT);

(c) **"Act"** means the Telecom Regulatory Authority of India Act, 1997 (24 of 1997)

(d) **"Authority"** means the Telecom Regulatory Authority of India established under sub-section (1) of section 3 of the Act;

(e) **"Auto Dialer Call"** means a call which is initiated automatically by an equipment, in accordance to a stored and/ or programmable instruction(s), to a telephone number(s), already stored or a list auto generated by the software, and once the call has been answered, equipment

(i) either plays a recorded message; or

(ii) connects the call to a live person;

(f) **"Bulk"** means number of messages or voice calls on the same or similar subject-matter sent, caused to be sent or authorized to be sent in excess of the following limits: -

(i) more than 20 during a twenty-four hours period; or

(ii) more than 100 during a seven days period; or

(iii) *more than 300 during a thirty days period;*

IndiaCode

(g) **"Business Day"** means any day other than a Saturday, Sunday and a Gazette holiday declared by the Central government;

(h) **"Calling Name or Number (CNAM)"** means name or number which is presented by the terminating access provider (TAP) to the recipient of a commercial communication which may be the header assigned to the sender or a name or number assigned by the access provider in lieu of header or number;

(i) **"Commercial Communication"** means any voice call or message using telecommunication services, where the primary purpose is to inform about or advertise or solicit business for

(A) goods or services; or
(B) a supplier or prospective supplier of offered goods or services; or
(C) a business or investment opportunity; or
(D) a provider or prospective provider of such an opportunity;

**Explanation:**

For the purposes of this regulation it is immaterial whether the goods, services, land or opportunity referred to in the content of the communication exist(s), is/are lawful, or otherwise. Further, the purpose or intent of the communication may be inferred from:

(A) The content of the communication in the message or voice call
(B) The manner in which the content of message or voice call is presented
(C) The content in the communication during call back to phone numbers presented or referred to in the content of message or voice call; or the content presented at the web links included in such communication.

(j) "**Consensus**" means the concurrence among the participants on a distributed ledger to record an irrevocable data value, which is cryptographically secured;

(k) **"Consent"** means any voluntary permission given by the customer to sender to receive commercial communication related to specific purpose, product or service. Consent may be explicit or inferred as defined in these regulations;

(l) **"Consent Acquirer or CA"** means any sender with registered and valid header(s), who acquires consent through a prescribed process under the relevant regulations;

(m) **"Consent Register"** means a Distributed Ledger for Consent (DL-Consent) having all relevant details of consent acquired by sender, in a secure and safe manner, to send commercial communications and may be required for the purpose of pre and post checks for regulatory compliance based on the consent;

(n) **"Consent Registrar or CR"** is an authorized entity under relevant regulations responsible for maintaining the consent register, customer consent acquisition facility and customer consent verification facility;

(o) **"Consent Template or CT"** means a template of content which is presented to the customer while acquiring his consent and clearly mentions purpose of the consent and details of sender;

(p) **"Consent Template Register"** means a Distributed Ledger for registration of Consent Template (DL-TCS) which keeps record of unique consent template identity along with the content of consent template and details of sender who got it registered, in a secure and safe manner;

(q) **"Content Template for Transaction"** means a template of content registered by any sender with the access provider for sending transactional message, service message or transactional voice call, service call for the purpose of commercial communication and contains content which may be a combination of fixed part of content and variable part of content, where

(i) fixed part of content is that part of content which is common across all commercial communications sent to different recipients for same or similar subject;

(ii) variable part of content is that part of content which may vary across commercial communications sent to different recipients for same or similar subject on account of information which is very specific to the particular transaction for a particular recipient or may vary on account of reference to date, time, place or unique reference number;

(r) **"Content Template for Promotion"** means a template of content registered by any sender with the access provider for sending promotional message or promotional voice call for the purpose of commercial communication and contains content which is fixed content and common across all commercial communications sent to different recipients for same or similar subject;

(s) **"Content Template Register"** means a Distributed Ledger for Content Template which keeps records of unique content template identity along with the content of content template and details of sender who got it registered in a safe and secure manner;

(t) **"Content Template Registrar"** is an authorized entity under the relevant regulations responsible for maintaining the Content template register and Content template registration facility;

(u) **"Customer"** means subscriber;

indiaCode

(v) **"Customer Preference Registration Facility or CPRF"** means the facility established by an Access Provider, under relevant regulations, for the purpose of registration, modifications or de-registration of the preference of its customers in respect of receipt of commercial communications;

(w) **"Distributed Ledger Technologies (DLT)"** means a set of technological solutions that enables a single, sequenced, standardized and cryptographically-secured record of activities to be safely distributed to, and acted upon, by a network of varied participants and their

(i) database can be spread across multiple sites or institutions;

(ii) records are stored one after the other in a continuous ledger and can only be added when the participants reach a consensus;

(x) **"Entity Register"** means a Distributed Ledger for Entities (DL-Entities) having a records of all entities registered to carry out telemarketing related function(s) with all relevant details.

(y) **"Explicit consent"** means such consent as has been verified directly from the Recipient in a robust and verifiable manner and recorded by Consent Registrar as defined under these regulations;

(z) **"Fully blocked"** means stoppage of all types of commercial communication requiring explicit consent except commercial communication sent under inferred consent;

(aa) **"Header"** means an alphanumeric string of maximum eleven characters or numbers assigned to an individual, business or legal entity under these regulations to send commercial communications;

(ab) **"Header Root"** means the common sub string of block of headers, starting from the first character;

(ac) **"Header Branch"** means the sub string of a header other than header root;

(ad) **"Header Registration Facility or HRF"** means the facility established by Header Registrar, under relevant regulations, for registration or de-registration of the header of any principal entity or content provider for sending commercial communications;

(ae) **"Header Register"** means a Distributed Ledger for Header (DL-Header) which keeps records of header(s), its purpose of sending commercial communications and details of sender to whom it is assigned in a safe and secure manner;

(af) **"Header Registrar"** is an authorised entity under relevant regulations responsible for maintaining the header register, header registration facility and header verification facility;

(ag) **"Immutable"** means data added to the distributed ledger after achieving consensus, which thereafter is unchangeable, secure and preserved for the life of the ledger;

(ah) **"Inferred Consent"** means any permission that can be reasonably inferred from the customer's conduct or the Relationship between the Recipient and the Sender;

IndiaCode

| | |
|---|---|
| (ai) | **"Message"** shall have the meaning assigned to it in clause (3) of section 3 of the Indian Telegraph Act, 1885 (13 of 1885); |
| (aj) | **"National Numbering Plan" (NNP)** means the National Numbering Plan issued by DoT from time to time; |
| (ak) | **"Node**" means participants on a distributed ledger having particular rights to read or write data; |
| (al) | **"Non-repudiable"** means<br>(i) making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use) so that an individual or entity cannot deny having performed a particular action;<br>(ii) ensuring the availability of evidence that can be presented to Authority and used to prove that some kind of event or action has taken place; |
| (am) | **"One Time Password or OTP"** means an automatically generated random number used to authenticate the action of user for a single transaction or session. |
| (an) | **"Originating Access Provider" (OAP)** means the Access Provider who has provided the telecom resources to a sender; |
| (ao) | **"Permissioned DLT networks**" means those DLT networks where participants in the process are preselected and addition of new record on the ledger is checked by a limited consensus process using a digital signature; |
| (ap) | **"Preference of Category of Commercial Communication"** means preference exercised by the customer to permit only a selected category of commercial communications out of available choices prescribed by relevant regulations; |
| (aq) | **"Preference of Mode for Commercial Communication"** means preference exercised by the customer to permit commercial communications only through the selected mode of communications from the choices for modes made available in the relevant regulations or code(s) of practice; |
| (ar) | **"Preference of Time band and Day type for Commercial Communication"** means preference exercised by the customer to permit unsolicited commercial communications only during time slots and type of days out of choices for time band(s) and types of day(s) made available in the relevant regulations; |
| (as) | **"Preference Register"** means a Distributed Ledger for Preference (DL-Preference) which keeps records of preference(s) of customers about category of content, mode(s) of communication, time band(s), type of day(s) along with the details of customer who has exercised choices of preference(s), day and time such choices or changes in choices were exercised in a safe and secure manner; |
| (at) | "**Private DLT networks**" means those DLT networks where visibility is restricted to a subset of users; |

IndiaCode

(au) **"Promotional messages"** means commercial communication message for which the sender has not taken any explicit consent from the intended Recipient to send such messages;

(av) **"Promotional voice call"** means commercial communication voice call for which the Sender has not taken any explicit consent from the Recipient to make such voice calls to him;

(aw) **"Recipient",** in relation to a commercial communication, means an authorised user of the telephone number(s) to whom the message is sent or voice call is made.

**Explanation:**

Where a recipient of a message or voice call has one or more Telephone numbers in addition to the Telephone number to which the message was sent or voice call was made, the recipient shall be treated as a separate recipient with respect to each such Telephone number;

(ax) **"Referred Telephone Number" (RTN)** means telephone number or telecom resource referred to in the content of commercial communication messages or voice calls from the sender;

(ay) **"Registered Telemarketer (RTM)"** means any telemarketer who is registered with the access provider(s) in accordance with the procedure and conditions specified in these regulations.

(az) **"Regulations"** means the Telecom Commercial Communications Customer Preference Regulations, 2018, unless otherwise indicated;

(ba) **"Regulatory Sandbox"** means specifically constructed experimental space, with a safe environment, within which various stakeholders can use Regulatory Technology solutions to develop and refine Code(s) of Practice to comply with new regulatory requirements;

(bb) **"Relationship"** means a prior or existing relationship

(i) for business or commercial reasons, between a person or entity and a subscriber with or without an exchange of consideration,

(ii) on the basis of the purchase or transaction made by or done by the recipient with the sender within the tweleve months immediately preceding the date of the communication; or

(iii) on the basis of inquiry or application regarding products or services made by or submitted by recipient to sender within the three months immediately preceding the date of the receiving of communication, which relationship has not been previously terminated by either party;

(iv) for social reasons, between a person or entity and a subscriber with or without an exchange of consideration, by voluntary two-way communication, initiated from both sides at different points in time;

(bc) **"Robo Calls"** means any call made to any customer using an artificial or prerecorded voice to interactively deliver a voice message without the involvement of human being on calling side for participating in the dialogue;

(bd) **"Scrubber"** means an entity registered with the access provider(s) and authorised by the relevant regulations to perform the function of scrubbing in accordance with the relevant

IndiaCode

regulations;

(be) **"Scrubbing"** means process of comparing target list of telephone number(s) provided by the Sender, to whom it wishes to send commercial communication with the list of telephone number(s) in DL-Preference and DL-Consent to check whether commercial communication(s) can be sent to the Recipient as per his registered preference(s) or as per consent;

(bf) **"Sender",** in relation to a commercial communication, means

(i) The person or entity who owns the telephone number or the header(s) that were used;

(ii) A person or entity that publicly asserts or uses a Calling Line Identity (CLI) or the phone number(s) referred to in the communication, except where such assertion is fraudulent;

(iii) The person who sent the message or made a voice call, caused the message to be sent or the voice call to be made or authorized the sending of the message or making of the voice call;

(iv) The person or legal entity dealing with goods, or services, or land or property, or a business or investment opportunity that is offered or promoted; except where such entity maintains a distinct legal identity for the division or line of business dealing with offered goods, services or opportunity, in which case such division or line of business;

(bg) **"Sender information or SI"** means the source, destination and routing information attached to a message or voice call, including, where applicable, the originator's name and originating phone number, reference telephone number, and any other information that appears in the content of commercial communication identifying, or purporting to identify, the sender of the message or making voice call;

(bh) **"Service message or Service Call"** means a message sent to a recipient or voice call made to recipient either with his consent or using a template registered for the purpose, the primary purpose of which is-

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously consented to enter into with the sender; or

(ii) to provide warranty information, product recall information, safety or security information with respect to a commercial product or service used or purchased by the recipient;

to provide—

(A) notification concerning a change in the terms or features of; or

(B) notification of a change in the recipient's standing or status with respect to; or

(C) at regular periodic intervals, account balance information or other type of account statement with respect to, a subscription, membership, account, loan, or comparable ongoing; or

(D) commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; or

(E) information directly related to an employment relationship or related benefit plan in which the Recipient is currently involved, participating, or enrolled; or

(F) information relating to delivery of goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously consented to enter into with the sender;

(bi) **"Signature"** means pattern in communications from particular telephone number(s) or telecom resource(s) or person, entity which are not registered with the access provider(s) for

InfraCode

| | |
|---|---|
| | commercial communication purposes and also includes pattern in communications from particular sender(s), who are registered with the access provider(s) but not authorised to send commercial communication of particular type or for specific purpose(s) which may require additional authorisations from relevant Government or statutory bodies to send such commercial communications; |
| (bj) | **"Silent Call"** means any unsolicited call made by a person or an entity to a customer for a very short duration in which either called party has not yet been alerted by his or her device, or it is very unlikely to be answered, wherein the intention of caller is to get call back from called party and then enter into commercial communication; |
| (bk) | **"Smart contract"** means a functionality of intelligent and programmable code which can execute pre-determined commands or business rules set to pre-check regulatory compliance without further human intervention and suitable for DLT system to create a digital agreement, with cryptographic certainty that the agreement has been honored in the ledgers, databases or accounts of all parties to the agreement; |
| (bl) | **"Smartphone"** means a device with large display, predominantly with touch screen technology, fast processor and memory in the GB range. A fully-featured Operating System or platform that provides voice and data communications capabilities, enables personalization of the device by the user and in addition supports installation and maintenance of mobile applications e.g., downloadable from an Application store. |
| (bm) | **"SMS"** means a message which is sent through short message service and includes a Multi-Media message which is sent through Multi-Media message service (MMS); |
| (bn) | **"Subscriber"** means a person or legal entity who subscribes to a telecom service provided by an Access Provider; |
| (bo) | **"Telecom resources"** means any telegraph used to send voice call or messages; |
| (bp) | **"Telemarketer"** means a person or legal entity engaged in the activity of transmission or delivery of commercial communication or scrubbing or aggregation. |
| (bq) | **"Telephone number"** means a number which may or may not have been assigned to the subscriber of a Public Switched Telecom Network (PSTN) or a wireless access network or a mobile network from a numbering series already assigned to a telecom service providers to which either an SMS or MMS can be sent, or Voice calls can be made.<br><br>**Explanation:** For the purposes of these regulations, it is immaterial whether the telephone number is actually assigned to any customer or not or has ceased to exist; |
| (br) | **"Telephone number harvesting software"** means software that is specifically designed or marketed for use in —<br>(i) searching the Internet, directories, contact lists in devices for telephone numbers; and<br>(ii) collecting, compiling, capturing or otherwise harvesting those telephone numbers;<br>(iii) generating most likely valid telephone numbers using automated means; |
| (bs) | **"Terminating Access Provider" (TAP)** means the Access Provider of which Recipient of |

mainCode

commercial communication is a Subscriber;

(bt) **"Transactional message"** means a message triggered by a transaction performed by the Subscriber, who is also the Sender's customer, provided such a message is sent within thirty minutes of the transaction being performed and is directly related to it.

Provided that the transaction may be a banking transaction, delivery of OTP, purchase of goods or services, etc.

(bu) **"Transactional Voice Call"** means a voice call which is not promotional in nature and is for the purpose of alerts to its own customers or account holders and information to be communicated by the voice call is time critical in the nature;

(bv) **"Unregistered Telemarketer" (UTM)** means any Sender of commercial communication who is not registered for the purpose of telemarketing with the access provider(s);

(bw) **"Unsolicited commercial communication or UCC"** means any commercial communication that is neither as per the consent nor as per registered preference(s) of recipient, but shall not include:

(i) Any transactional message or transactional voice call;

(ii) Any service message or service voice call;

(iii) Any message or voice calls transmitted on the directions of the Central Government or the State Government or bodies established under the Constitution, when such communication is in Public Interest;

(iv) Any message or voice calls transmitted by or on the direction of the Authority or by an agency expressly authorized for the purpose by the Authority.

(bx) **"Usage Cap"** means a limit put on a telephone number for making a maximum of twenty outgoing voice calls per day and a maximum of twenty outgoing messages per day.

**CHAPTER-II**

**COMMERCIAL COMMUNICATION THROUGH ACCESS PROVIDER NETWORK**

3. Every Access Provider shall ensure that any commercial communication using its network only takes place using registered header(s) assigned to the sender(s) for the purpose of commercial communication; and

(1) No Subscriber, who is not registered with any access provider for the purpose of sending commercial communications under these regulations, shall make unsolicited commercial communication and

(a) in case, any Subscriber is sending Commercial Communication, telecom resources of the sender may be put under usage cap; and

(b) if the Subscriber continues to send Commercial Communication despite notice given to him under these regulations, all telecom resources of the sender may also be disconnected;

4. No Sender registered for making commercial communication shall initiate calls with an Auto dialer that may result in silent or abandoned calls.

IndiaCode

Provided that the sender has notified the originating access provider in advance about the use of the auto dialer and taken steps to maintain abandoned calls within limits provided for in these regulations or Code(s) of Practice.

5. Every Access Provider shall develop or cause to develop an ecosystem with the following functions to regulate the delivery of the commercial communications as provided for in these regulations: -

(1) to provide facility to its Subscribers for registering preference(s) for Commercial Communication and maintain complete and accurate records of preference(s);

(2) to register entities for participating in the ecosystem and prescribe their roles and responsibilities for efficient and effective control of commercial communications;

(3) to provide facility to record consent(s) of the Subscribers acquired by the sender(s) for sending Commercial Communication and maintain complete and accurate records of consent(s);

(4) to provide facility for revocation of consent by its Subscribers and accordingly update records of consent for the Subscribers;

(5) to register sender(s), carry out verifications of their identities and prescribe processes for sending commercial communications;

(6) to prescribe process and specific functions of particular entity to carry out pre-delivery checks before sending commercial communications and ensuring regulatory compliance(s);

(7) to provide facilities for its Subscribers to register complaints against Sender(s) of Commercial Communication and maintain complete and accurate records of status of resolution of complaints;

(8) to examine and investigate complaints, take actions against defaulters and take remedial measures to ensure compliance with the regulations;

(9) to detect, identify and act against sender(s) of Commercial Communication who are not registered with them;

(10) to comply with any other directions, guidelines and instructions issued by the Authority in this regard.

**CHAPTER-III**

**CUSTOMER PREFERENCE REGISTRATION**

6. **Every Access Provider shall establish Customer Preference Registration Facility (CPRF) and shall make necessary arrangements to facilitate its customers, on 24 hours X 7 days basis throughout the year:**

(1) to provide ways and means to record consent or record revocation of consent related to Commercial Communication and exercise his preference(s) from the list(s), mentioned in the Schedule-II, of choices for: -

(a) preference(s) of categories of Commercial Communication;

(b) preference(s) of the mode(s) of communication,

(c) preference(s) of time band(s) and types of day(s) of the week including public and national holidays;

(2) to provide following modes, free of cost, to the customer, as per his choice, to register, modify or

IndiaCode

de register preference(s): -

(a) sending SMS to short code 1909; or

(b) calling on 1909; or

(c) Interactive Voice Response System (IVRS); or

(d) sending USSD; or

(e) Mobile app developed in this regard either by the Authority or by any other person or entity and approved by the Authority; or

(f) Web portal with authentication through OTP; or

(g) Any other means as may be prescribed by the Authority from time to time.

(3) to duly acknowledge the receipt within fifteen minutes of the request made by the customer for registering, modifying, deregistering the preference with unique reference number;

7. Every Access Provider shall ensure that preferences recorded or modified by the Subscriber are given effect to in near real time and in such a manner that no delivery of commercial communication is made or blocked in contravention to the Subscribers' preference after twenty-four hours or such time as the Authority may prescribe.

**CHAPTER-IV**

**FUNCTIONS OF ACCESS PROVIDERS**

8. Every Access Provider shall undertake following activities in accordance with the provisions of these regulations before allowing any commercial communication through its network(s): -

(1) Develop Code(s) of Practice to establish system and make arrangements to govern the specified activities: -

(a) Code of Practice for Entities of ecosystem (CoP-Entities) as per Schedule-I;

(b) Code of Practice for Registration of preference(s), recording consent(s) and revocation of consent(s) (CoP-Preference) as per Schedule-II;

(c) Code of Practice for Complaint Handling (CoP-Complaints) as per Schedule-III;

(d) Code of Practice for Unsolicited Commercial Communications Detection (CoP-UCC_Detect) as per Schedule-IV;

(e) Code of Practice for monthly reporting (CoP-Reports) as per Schedule-V

(2) Register entities as provided for in Code(s) of Practice for Entities

(3) Register Sender(s) and assign the header(s), header root(s);

(4) Register the Content Templates;

(5) Register the Consent Templates;

9. Every Access Provider shall ensure that no commercial communication is made to any Recipient, except as per the preference(s) or digitally registered consent(s) registered in accordance with these regulations.

IndiaCode

10. Every Access Provider shall ensure that no commercial communication takes place through its network(s) except by using header(s) assigned to the registered Sender(s) for the purpose of sending commercial communication;

11. Every Access Provider shall give due publicity through appropriate means to make the customers aware regarding: -

(1) The procedure(s) and facilities for registering preference(s);

(2) The procedure(s) and facilities for registration and revocation of Consent(s);

(3) The procedure(s) and facilities for making complaint(s), providing information or reporting Unsolicited Commercial Communication;

(4) Every Access provider shall inform its Subscribers while giving telecom resources that he shall not get involved in the activity of sending Commercial Communication or cause sending Commercial communication, or authorize the sending of the Commercial Communication using the telecom resources failing which the telecom resources used or assigned to him may be put under Usage Cap or his telecom resources may be disconnected;

Provided that the Authority may, from time to time, issue such directions as it deems necessary, specifying the content, medium, frequency and manner of such publicity;

**CHAPTER-V**

**OBLIGATIONS OF ACCESS PROVIDERS**

IndiaCode

12. Access Providers shall deploy, maintain and operate a system, by themselves or through delegation, to ensure that requisite functions are performed in a non-repudiable and immutable manner: -

(1) to record preference(s), consent(s), revocation of consent(s), complaint(s) etc.

(2) to carry out regulatory pre-checks and post-checks in respect of Commercial Communication being offered for delivery and also to keep records of actions performed;

(3) to register person(s), business entity(ies) or legal entity(ies) in making Commercial Communication through its network involved from origination, transmission or delivery and have adequate documentary evidence in support to prove its identity;

(4) to ensure that functions and actions performed by registered entities are identifiable, distinguishable and recordable;

(5) to ensure that the data is stored and shared in a secure and safe manner;

(6) to ensure that data is accessible only to the relevant entities for performing roles assigned to them under these regulations;

*Note:* If not specifically permitted, the data should not be accessible in clear text to any person, including the person(s) operating the system or performing a delegated function, e.g. scrubbing, or accessible to any application(s) other than the application performing the delegated function(s).

(7) to detect non-compliances and take immediate action to effectively ensure compliance with regulations;

(8) to ensure compliance by the registered sender(s) who have notified the access provider about the use of auto dialer(s), and to take action against the sender(s) found to be failing to maintain silent

| |
|---|
| calls or abandoned calls within the prescribed limits; |
| 13. Access Providers shall adopt Distributed Ledger Technology (DLT) with permissioned and private DLT networks for implementation of the system, functions and processes as prescribed in Code(s) of Practice:<br>(1) to ensure that all necessary regulatory pre-checks are carried out for sending Commercial Communication;<br>(2) to operate smart contracts among entities for effectively controlling the flow of Commercial Communication; |
| 14. Access Providers may authorise one or more DLT network operators, as deemed fit, to provide technology solution(s) to all entities to carry out the functions as provided for in these regulations. |
| 15. Every Access Provider shall develop the prescribed Code(s) of Practice, if necessary, in collaboration with other Access Providers, including relevant stakeholders required to participate to carry out the functions provide for in these regulations. |
| 16. The Access Providers shall submit the Code(s) of Practice (CoPs) to the Authority within three months from the date of coming into force of these regulations. |
| 17. Authority may direct Access Provider(s) to make changes, at any time, in the Code(s) of Practice and Access Providers shall incorporate such changes and submit revised CoP within fifteen days from the date of direction issued in this regard. |
| 18. Every Access Provider shall comply with the submitted Codes of Practices and implement them in accordance with the specified time line(s),<br>Provided that any provision in Code(s) of Practice shall not have effect to the extent of being inconsistent with these regulations. |
| 19. The Authority reserves the right to formulate a standard Code(s) of Practice in case the formulated CoP is deficient to serve the purposes of these regulations. |
| 20. Every access provider shall comply with the provisions of Standard Code(s) of Practice. |
| 21. In case of non-compliance to the provisions of Code(s) of Practice, Access Provider shall be liable to pay, by way of financial disincentive, following amount: -<br>(1) not exceeding Rupees five thousand per day for the period of exceeding the timeline if the period of delay is less than or equal to thirty days;<br>(2) not exceeding Rupees twenty thousand per day for the additional period of delay which is more than thirty days;<br>The amount payable by way of financial disincentive under these regulations shall be remitted to such head of account as may be specified by the Authority.<br>The total amount payable as financial disincentives under sub-regulations (1) and (2) shall not exceed rupees ten lakhs.<br>The Authority reserves the right not to impose financial disincentive or to impose a lower amount of |

IndiaCode

financial disincentive or no incentive where it finds merit in the reasons furnished by the access provider.

Provided that no order for payment of any amount by way of financial disincentive shall be made by the Authority, unless the concerned Access Provider has been given a reasonable opportunity to represent.

22. **Prescription of fee/ charges by Access Providers:** Access Providers may prescribe fee from participating entities for sending commercial communications for registration and to carry out activities provided for in these regulations and may also prescribe security deposits. Access providers may impose financial disincentive on participating entities in case violation of regulations can be attributed to failure of functions assigned to such entities.

**CHAPTER-VI**

**COMPLAINT REDRESSAL**

23. **Every Access Provider shall establish Customer Complaint Registration Facility (CCRF) and shall make necessary arrangements to facilitate its customers on 24 hours X 7 days basis throughout the year**: -

(1) to provide ways and means: -

(a) to make complaint(s), by its customer who has registered his preference(s), against sender(s) of unsolicited commercial communication in violation of the registered preferences or digitally registered consents;

(b) to submit report(s), against sender(s) of commercial communication in violation of provisions of these regulation(s) by any customer;

(2) to provide following modes, as per choice of the customer and free of cost, to make complaint or to report violation of regulations: -

(a) sending SMS to short code 1909; or

(b) calling on 1909; or

(c) Interactive Voice Response System (IVRS); or

(d) Mobile app developed in this regard either by the Authority or by any other person or entity and approved by the Authority; or

(e) Web portal with authentication through One Time Password (OTP); or

(f) Any other means as may be notified by the Authority from time to time.

*Provided that* every such complaint shall be made by a subscriber within three days of receipt of the unsolicited commercial communication;

(3) to duly acknowledge the receipt within fifteen minutes of the complaint or report made by the customer with unique reference number;

(4) to provide details to the subscriber about the mobile app provided for in sub-regulation (2)(d)

(5) to provide details about format and procedure to the customer, as given in the appropriate Code(s) of Practice, where a complaint is rejected by the access provider on the grounds of incomplete information or improper format;

24. **Distributed Ledger(s) for Complaints:** Every Access Provider shall establish or cause to establish

IndiaCode

Distributed Ledger(s) for Complaints (DL-Complaints) with requisite functions, processes and interfaces: -

(1) to record complaints and reports regarding violation of Regulations made by the customer in the Distributed Ledger for Complaints (DL-Complaints) in an immutable and non repudiable manner;

(2) to record, at least, following details about the complaint or report regarding violation of Regulations:

(a) telephone number(s) or header(s) from which Unsolicited Commercial Communication was received;

(b) telephone number(s) of Complainant or reporter;

(c) Referred telephone number(s) (RTN), if any;

(d) Date and time of occurrence of Unsolicited Commercial Communication, if available;

(e) unique registration number issued at the time of making complaint or reporting;

(f) resolution status of the complaint or report regarding violation of Regulations;

(3) to record three years history of complainant with details of all complaint(s) made by him, with date(s) and time(s), and status of resolution of complaints;

(4) to record three years history of sender(s) against which complaint is made or reported with details of all complaint(s), with date(s) and time(s), and status of resolution of complaints;

(5) to interact and exchange information with other relevant entities in a safe and secure manner;

(6) to support any other functionalities as required to carry out functions provided for in these regulations;

IndiaCode

25. **Complaint Mechanism:** Every Access Provider shall establish system(s), functions and processes to resolve complaints made by the customers and to take remedial action against sender(s) as provided hereunder:

(1) Terminating Access Provider (TAP) shall record the complaint on DL-Complaints in non-repudiable and immutable manner and shall notify, in real time, the details of the complaint to the concerned Originating Access Provider (OAP).

(2) Terminating Access Provider (TAP) shall examine within one business day from the date of receipt of complaint, to check the occurrence of complained communication between the complainant and the reported telephone number or header from which unsolicited commercial communication was received and update the findings on DL-Complaints.

(3) Terminating Access Provider shall also verify if the date of receipt of complaint is within three days of receiving commercial communication and in case the complaint is reported by the customer after three days, the TAP shall communicate to the customer about the closure of his complaint in accordance to the Code of Practice for Complaint Handling and change status of complaint on DL-Complaint as a report instead of complaint.

(4) The OAP, in case the complaint is related to RTM, shall examine, within one business day from the date of receipt of complaint, whether all regulatory pre-checks were carried out in the reported case before delivering Unsolicited Commercial Communications; and

(a) In case, all regulatory pre-checks were carried out and delivery of commercial communication to the recipient was in confirmation to the provisions in the regulations and Code(s) of Practice,

OAP shall communicate to TAP to inform complainant about the closure of complaint as provided for in the Code(s) of Practice;

(b) in case of non-compliance with the regulations, the OAP shall, within two business days from the date of receipt of complaint, take actions against the defaulting entity and communicate to TAP to inform the complainant about the action taken against his complaint as provided for in Code(s) of Practice;

(c) the OAP shall take appropriate remedial action, as provided for in the Code of Practice(s), to control Unsolicted Commercial Communications so as to ensure compliance with these regulations;

(5) The OAP, in case, the complaint is related to a UTM,

(a) shall examine communication detail records (CDRs), within one business day from the date of receipt of complaint, to check the occurrence of complained communication between the complainant and the reported telephone number or header from which unsolicited commercial communication was received.

(b) In case of no occurrence of complained communications under sub-regulation (5)(a), OAP shall communicate to the TAP to inform the complainant about the closure of complaint in a manner prescribed in the Code(s) of Practice;

(c) In case of occurrence of complained communications under sub-regulation (5)(a), OAP shall further examine, within two business days from the date of complaint, whether there are similar complaints or reports against the same sender; and

(i) *in case, it is found that number of complaints against the sender are from ten or more than ten recipients over a period of last seven days, the OAP shall put sender under Usage Cap and at the same time shall initiate investigation as provided for in sub-regulation (6);*

Provided that *such Usage Cap shall be valid till investigation is completed or thirty days from the date of effect of restrictions, whichever is earlier;*

(ii) *in case it is found that number of complaints against the sender are from less than ten recipients over a period of last seven days, the OAP shall, from the previous thirty days data of CoP_UCC_Detect System, check whether suspected sender is involved in sending Commercial Communication in bulk or not; and*

(A) in case, sender has sent commercial communications in bulk, the OAP shall put the sender under Usage Cap, and at the same time initiate investigation as provided for in sub-regulation (6);

*Provided that* such restrictions shall be valid till investigation in this regard is completed under relevant regulations or thirty days from the date of effect of restrictions, whichever is earlier;

(B) in case, sender has not sent commercial communications in bulk, the OAP shall warn such sender through appropriate means as provided for in Code(s) of Practice;

(6) OAP shall issue notice, within three business days, to give opportunity to such sender(s), under sub regulations (5)(c)(i), (5)(c)(ii)(A) to represent his case and shall investigate, within thirty business days from the date of receipt of complaint and shall conclude whether the communication so made was unsolicited commercial communication or not; and conclusion of the investigation was that sender was engaged in sending unsolicited commercial communications, OAP shall take action against such sender as under: -

(a) for first instance of violation, due warning shall be given;

TRAI Code

*Provided that* the first instance of the violation shall include all the complaints against the sender within two business days after the date of receipt of the first complaint, against which the sender is to be warned under this sub-regulation.

(b) for the second instance of violation, Usage Cap shall continue for a period of six months;

*Provided that* the second instance of the violation shall include all the complaints against the sender after the issuance of first warning within two business days after the date of receipt of the complaint against which second warning is being given to the sender under this sub-regulation.

(c) for third and subsequent instances of violations, all telecom resources of the sender shall be disconnected for a period up to two years and OAP shall put the sender under blacklist category and communicate to all other access providers to not to allocate new telecom resources to such sender for up to two years from the date of such communication;

*Provided that* the third instance of the violation shall include all the complaints received against the sender after the date of second warning within two business days after the receipt of the complaint against which telecom resources are being disconnected under this sub-regulation.

*Provided further that* one telephone number may be allowed to be retained by such sender with the Usage Cap for a period up to two years.

IndiaCode

26. **Record keeping and reporting:**

(1) Every Access Provider shall maintain records of complaints, from its customers and received from Terminating Access Provider(s), against registered sender(s) for sending unsolicited commercial communications on daily basis for each service area and submit performance monitoring report to the Authority as and when required in a format as prescribed.

(2) Every Access Provider shall maintain records of complaints, from its customers and received from Terminating Access Provider(s), against unregistered sender(s) for sending unsolicited commercial communications on daily basis for each service area and submit performance monitoring report to the Authority as and when required in a format as prescribed.

(3) Every Access Provider shall submit to the Authority its compliance reports in respect of unsolicited commercial communications, complaints or reports from its customers in such manner and format, at such periodic intervals and within such time limits as may be specified by the Authority, from time to time, by an order or direction;

(4) The Authority may, from time to time, through audit conducted either by its own officers or employees or through agency appointed by it, verify and assess the process followed by the access provider for registration and resolution of complaints, examination and investigation of the complaints and reporting to the Authority.

27. Consequences for the Originating Access Provider (OAP) failing to curb the unsolicited commercial communications sent through its network(s): -

(1) If OAP fails to curb UCC, Financial Disincentives for not controlling the Unsolicited Commercial Communications (UCC) from RTMs by the access provider in each License Service Area for one calendar month shall be as under: -

| | Value of "Counts of UCC for RTMs for one calendar month" | Amount of financial disincentives in Rupees |
|---|---|---|

| | | |
|---|---|---|
| (a) | More than zero but not exceeding hundred | Rupees one thousand per count |
| (b) | More than hundred but not exceeding one thousand | Maximum financial disincentives at (a) plus Rupees five thousand per count exceeding hundred |
| (c) | More than one thousand | Maximum financial disincentives at (b) plus Rupees ten thousand per count exceeding one thousand |

*Provided* that no order for payment of any amount by way of financial disincentive shall be made by the Authority, unless the concerned Access Provider has been given a reasonable opportunity to represent.

*The* amount payable by way of financial disincentive under these regulations shall be remitted to such head of account as may be specified by the Authority.

(2) The total amount payable as financial disincentives under sub-regulations (1) shall not exceed rupees fifty lakhs per calendar month. The Authority may impose no financial disincentive or a lower amount of financial disincentive than the amount payable as per the provisions in sub-regulation (1) where it finds merit in the reasons furnished by the access provider.

28. **Consequences for contravention of the provisions of regulations by Access Providers: -**

(1) **Power of Authority to order inquiry:** -

(a) Where the Authority has a reason to believe that any Access Provider has contravened the provisions of these regulations, it may constitute an inquiry committee, to inquire into the contravention of the regulations and to report thereon to the Authority.

(b) The inquiry committee shall give a reasonable opportunity to the concerned Access Provider to represent itself, before submitting its findings to the Authority.

(2) If on inquiry, under sub-regulation (1), the Access Provider is found to have misreported the count of UCC for RTMs, it shall, without prejudice to any penalty which may be imposed under its licence or other provisions under these regulations, be liable to pay, by way of financial disincentive, an amount

(a) ten times the difference between disincentive computed by the Inquiry Committee and that computed earlier based on service provider's data, or Rs 5 lakhs, whichever is higher; and

Provided that in case of second and subsequent contraventions, to pay an amount equal to twice that of computed financial disincentives under this sub-regulation

(b) one lakh per instance for access provider found to be not imposing timely restrictions on outgoing usage of unregistered sender(s) in accordance with provisions in regulations 25(5) and 25(6);

*Provided* that no order for payment of any amount by way of financial disincentive shall be made by the Authority, unless the concerned Access Provider had been given a reasonable opportunity of representing against the findings of the inquiry committee.

The amount payable by way of financial disincentive under these regulations shall be remitted to such head of account as may be specified by the Authority.

The total amount payable as financial disincentives under sub-regulations (2)(a) and (2)(b) shall

IndiaCode

not exceed rupees ten lakhs in a week.

(3) The Authority may impose no financial disincentive or a lower amount of financial disincentive than the amount payable as per the provisions in sub-regulations (2)(a) and 2(b) where it finds merit in the reasons furnished by the access provider.

29. **Examination of telecom resources put under outgoing Usage Cap or having been disconnected: -**

(1) The Authority may, if it considers expedient to do so, on receipt of complaint, call for the details of the telecom resources put under Usage Cap or disconnected under the regulations 25(5) and 25(6), on account of unregistered telemarketing activity under and upon examination, for reasons to be recorded,

(a) If the Authority finds that conclusion of investigation lacks adequate evidence against the sender, it may direct the Access Provider to remove such restrictions on usage or restore all telephone number(s) of the person and delete the name and address of such customer(s) or sender(s) from the blacklist.

(b) If the customer or the Sender whose telecom resources have been put under restriction or disconnected on account of adequate evidence against the sender, makes a request, within sixty days of such action, to the Authority for restoring his telecom resources or removing the restrictions on usage and satisfies the Authority that it has taken reasonable steps to prevent recurrence of such contravention, the Authority may by order ask access provider(s) to remove such restrictions on usage or restore all telephone number(s) of the person and delete the name and address of such Sender(s) from the blacklist, as the case may be, on payment of an amount of five thousand rupees per resource to the Authority for restoration of all such telecom resources, subject to the condition that the total amount payable by the customer or sender shall not exceed rupees five lakhs.

Provided *that* the Authority may impose no financial disincentive or impose a lower amount where it finds merit in the reasons furnished by the customer.

**MIGRATION OF EXISTING REGISTERED ENTITIES AND RECORDS**

30. Access providers shall prepare migration plan for existing data, process and role being played at present by different entities to the new system of data, process and role of new entities prescribed in these regulations;

31. List of key activities (but not an exhaustive list) for preparation of migration plan, attached are as per schedule-VI;

**CHAPTER-VII**

**MISCELLANEOUS**

32. No business or legal entity not registered with the access provider for the purpose of sending commercial communications under these regulations shall make commercial communication or cause such message to be sent or voice call to be made or authorize the sending of such message or making of a voice call;

33. Power to appoint inquiry committee:

trai.gov

(1) Where the Authority has a reason to believe that any Sender of commercial communications on behalf of business or legal entities has contravened the provisions of these regulations, it may constitute an inquiry committee, to inquire into the contravention of the regulations and to report thereon to the Authority.

(2) The inquiry committee shall give a reasonable opportunity to the concerned entities to represent itself, before submitting its findings to the Authority.

(3) In case, it is found by the Inquiry committee set up in this regard that particular business or legal entity is engaged in sending commercial communications in contravention to the provisions of these regulations, the Authority may order or direct access provider(s) to disconnect all telecom resources or put all telecom resources of such business or legal entity under Usage Cap of such telecom resources for the period up to two years;

*Provided that* if such entity maintains a distinct legal identity for the division or line of business dealing with offered goods, services or opportunity, the Usage Cap or disconnection of telecom resources shall be limited to resources pertaining to such division or line of business;

*Provided* further that no order or direction shall be made by the Authority, unless the concerned business or legal entity had been given a reasonable opportunity to represent against the findings of the inquiry committee.

34. Every Access Provider shall ensure, within six months' time, that all smart phone devices registered on its network support the permissions required for the functioning of such Apps as prescribed in the regulations 6(2)(e) and regulations 23(2)(d);

Provided that where such devices do not permit functioning of such Apps as prescribed in regulations 6(2)(e) and regulations 23(2)(d), Access Providers shall, on the order or direction of the Authority, derecognize such devices from their telecom networks.

Provided further that no order or direction of derecognition of devices shall be made by the Authority unless the concerned parties have been given a reasonable opportunity of representing against the contravention of regulations observed by the Authority.

35. Terminating Access Provider (TAP) may charge Originating Access Provider (OAP) for Commercial communication messages as following: -

(1) Upto Rs. 0.05 (five paisa only) for each promotional SMS;

(2) Upto Rs. 0.05 (five paisa only) for each service SMS;

Provided that there shall be no Service SMS charge on: -

(i) *any message transmitted by or on the directions of the Central Government or State Government;*

(ii) *any message transmitted by or on the directions of bodies established under the Constitution;*

(iii) *any message transmitted by or on the directions of the Authority;*

(iv) *any message transmitted by any agency authorized by the Authority from time to time;*

36. Authority may set up or permit to set up a Regulatory Sandbox for testing implementation of regulatory checks using DLT networks and other technological solutions complementing DLT network(s) and to operationalize such regulatory sandbox, the Authority may, by order or direction, specify the requisite processes.

IndiaCode

| | |
|---|---|
| 37. | Every Access Provider and International Long Distance Operators shall ensure that no international incoming SMS containing alphanumeric header or originating country code +91 is delivered through its network.<br><br>Provided that Authority may issue directions as it deems necessary to control bulk international messages from time to time. |
| 38. | Repeal and Saving. - Save as provided hereunder, The Telecom Commercial Communications Customer Preference Regulations, 2010 (6 of 2010) are hereby repealed. Notwithstanding the repeal of the Telecom Commercial Communications Customer Preference Regulations, 2010 (6 of 2010), -<br><br>(a) anything done, or any action taken or purported to have been done under the said regulations shall be deemed to have been done or taken under the corresponding provisions of these regulations;<br><br>(b) the provisions contained in regulations 2 to 13, 16 to 20, 21 and 22 of the Telecom Commercial Communications Customer Preference Regulations, 2010 (6 of 2010) shall remain in force until these regulations come into force in their entirety. |

IndiaCode

(Sunil Kumar Gupta)

Secretary

**Note:** The Explanatory Memorandum explains the objects and reasons of the Telecom Commercial Communications Customer Preference Regulations 2018.

**Schedule-I**

**Action Items for preparing Code of Practice for Entity(ies) (CoP-Entities)**

1. Entity Registration Functionality:

(1) All entities with associated functions, who will be carrying out given functions for effective control of Unsolicited Commercial Communications being delivered through them, shall be declared by each Access Provider on their websites;

(2) any individual, business entity or legal entity may carry out one or more functions while keeping all records and execution of functions separately against each activity for internal audit by the access provider to ensure the effectiveness of Unsolicited Commercial Communications control to meet regulatory outcomes specified in the regulations;

(3) each functional entity shall be given unique identity by the access provider(s) to be used to authenticate and track the events;

2. Every Access Provider shall formulate structure and format for headers to be assigned Senders for the purpose of commercial communications via sending SMS or making voice calls to participants which shall include following: -

(1) SMS Header, SMS Header Root, SMS Header Branch for Senders sending Promotional SMS, Transactional SMS and Service SMS from 11-character alphanumeric strings which are not allocated or assigned by DoT for other purpose(s) or in accordance to directions of the Authority/ DoT;

(2) Calling Line Identity for Senders making Promotional Voice Calls, Transactional Voice Calls and Service Voice Calls from 140-level numbering series or any other numbering series directed by the Authority/DoT;

IndiaCode

3. Every Access Provider shall formulate Code of Practice for Entities (CoP-Entities) involved from registered sender(s) to recipient(s) and

(1) CoP-Entities shall include at least following entities: -

(a) Header Registrar;

(b) Consent Registrar;

(c) Consent Template Registrar;

(d) Content Template Registrar;

(e) Content Template Verifier;

(f) Telemarketer Functional Entity Registrar for various functions prescribed in the relevant regulation(s);

(g) timeline(s) for implementation of the functionality referred in code of practice and operationalizing it;

(h) such other matters as the Authority may deem fit, from time to time;

(2) CoP-Entities shall also include at least following Distributed Ledger Nodes for the purpose of: -

(a) Header Register;

(b) Consent Register;

(c) Consent Template Register;

(d) Content Template Register;

(e) Content Template Verifier;

(f) Complaint Register;

(g) Preference Register;

(h) Telemarketer Scrubbing Function Register;

(i) Telemarketer Message Delivery Function Register;

(j) Telemarketer Voice Delivery Function Register;

(3) CoP-Entities shall include at least following: -

(a) implementation details for all functional entities;

(b) additional measures, as deemed fit by access provider(s), for functional entities required to ensure regulatory compliance;

(c) minimum standards of technical measures to effectively control the sending of unsolicited commercial electronic messages;

(d) technical mechanism to make available latest version of relevant and reliable data for an entity to carry out its desired function;

(e) such other matters as the Authority may deem fit, from time to time.

4. Every Access Provider shall carry out following functions: -

(1) Header Registration Function (HRF)

(a) assign header or Header root for SMS via Header Registration Functionality, on its own or through its agents, as per allocation and assignment principles and policies, to facilitate content provider or principal entity to get new headers;

(b) carry out pre-verifications of documents and credentials submitted by an individual, business entity or legal entity requesting for assigning of the header;

(c) bind with a mobile device and mobile number(s), in a secure and safe manner, which shall be used subsequently on regular intervals for logins to the sessions by the header assignee;

(d) carry out additional authentications in case of a request for headers to be issued to SEBI registered brokers or other entities specified by Authority by directions, orders or instructions issued from time to time;

(e) carry out additional authentications in case of a request for headers to be issued to government entities, corporate(s) or well-known brands, including specific directions, orders or instructions, if any, issued from time to time by the Authority;

(f) carry out additional checks for look-alike headers which may mislead to a common recipient of commercial communication, it may also include proximity checks, similarity after substring swaps specifically in case of government entities, corporate(s), well-known brands while assigning headers irrespective of current assignments of such headers, and to follow specific directions, orders or instructions, if any, issued from time to time by the Authority;

(2) Consent Registration Function (CRF)

(a) record consent via Customer Consent Acquisition Functionality on Consent Register, on its own or through its agents, to facilitate consent acquirers to record the consent taken from the customers

IndiaCode

in a robust manner which is immutable and non-repudiable and as specified by relevant regulations;

(b) Presenting content of consent acquisition template to the customer before taking consent;

(c) Taking agreement to the purpose of consent and details of sender;

(d) Authenticate customer giving the consent through OTP;

(e) record revocation of consent by the customer via revoke request in a robust manner which is immutable and non-repudiable and as specified by relevant regulations;

(f) record sufficient contact information, valid for at least 30 days, required to revoke consent and present it to recipient to enable them to submit request for revoking consent;

(3) Content Template Registration Function (CTRF)

(a) to check content of the template being offered for registration as a transactional template and service message template;

(b) to identify fixed and variable portion(s) of the content in the offered transactional template and service message template with identification of type of content for each portion of variable part of the content, e.g. date format, numeric format, name of recipient, amount with currency; reference number, transaction identity;

(c) to estimate the total length of variable portion, viz. total length of fixed portion for a typical transactional message, service message for offered template;

(d) to de-register template or temporarily suspend use of template;

(e) to generate one-way hash for fixed portion of content of template and ways to extract fixed portion and variable portion(s) from actual message for carrying out pre and post checks of actual content of actual message offered for delivery or already delivered;

(f) to check content of the template being offered for registration as a promotional from perspective of content category;

(g) assigning unique template identity to registered template of content;

(4) Scrubbing function (SF)

(a) to process scrubbing as defined, in a secure and safe manner, using preferences and consent of customer(s) and category of content;

(b) provide details about preferred time slots and types of days for delivery;

(c) take necessary measures to protect Preference Register and Consent Register data during scrubbing, e.g. by Generating virtual identities and tokens for each number for the messages and voice calls and not disclosing real identities to any other entity than authorized to know it;

(d) make available relevant details of scrubbed list to corresponding OAPs and TAPs for carrying out reverse mapping of virtual identities to real identities for further delivery;

(e) to identify and report probable instances of request received for scrubbing of list of phone numbers collected through harvesting software or instances of dictionary attack to relevant entities authorized to take action;

(5) Content Verification Function (CVF)

(a) to identify the content type and category of messages to be delivered or already delivered via an automated tool or utility software;

IndiaCode

(6) Delivery Function for Messages with Telecom Resource Connectivity to Access Provider (DF)

(a) deliver messages to OAP, in a secure and safe manner, during specified time slots and types of days of delivery in accordance to the preferences of the customer(s);

(b) select OAP for particular customer(s) or messages and conveying to Scrubber for generating tokens for corresponding OAP to access information of list of messages which would be required to be delivered by it;

(7) Aggregation Function for Message to other Telemarketer for delivery function (AF)

(a) deliver messages to RTM having telecom resource connectivity with access provider(s), in a secure and safe manner;

(8) Voice Calling Function with Telecom Resource Connectivity (VCF)

(a) deliver voice calls to OAP, in a secure and safe manner, during specified time slots and types of days of delivery in accordance to the preferences of the customer(s);

(b) select OAP for particular customer(s) or voice calls and conveying selected OAPs to Scrubber for generating tokens for corresponding OAP to access information of list of messages which would be required to be delivered by it;

5. Every Access Provider shall set up following functional entities or may delegate roles to perform following functions: -

(1) Header Registrar (HR) to

(a) establish and maintain header register as distributed ledger to keep headers, in a secure and safe manner, and make accessible relevant information for identifying the assignee at the time of request to carry out various functions, e.g. scrubbing function from the registered telemarketers for scrubbing, delivery function from telemarketer;

(b) carry out Header Registration Function;

(c) keep record of headers throughout its lifecycle, i.e. free for assignment, assigned to an entity, withdrawn, surrendered, re-assigned etc.;

(d) keep record of header(s), header root(s) reserved for specific purpose;

(e) synchronize records, in real time, among all header ledgers available with participating nodes in Header Registration Functionality in an immutable and non-repudiable manner;

(f) maintain with minimum performance requirements as specified;

(g) perform any other function and keep relevant details required for carrying out pre and post checks for regulatory compliance;

(2) Consent Registrar (CR) to

(a) establish and maintain consent register as distributed ledger to keep consent, in a secure and safe manner, and make accessible relevant data for scrubbing function to the registered telemarketers for scrubbing;

(b) establish Customer Consent Acquisition Facility (CCAF), to record recipient's consent to receive commercial communications from the sender or consent acquirer;

(c) establish Customer Consent Verification Facility (CCVF) for the purpose of facilitating:

(i) *customers to verify, modify, renew or revoke their consent in respect of commercial*

IndiaCode

*communications, and*

(ii) *Access Providers to verify the consent in case of complaint;*

(d) keep consent for each consent acquirer, in a manner that client data of entity is adequately protected;

(e) keep record of revocation of consent by the customer, whenever exercised, in an immutable and non-repudiable manner;

(f) synchronize records, in real time, among all consent ledgers available with participating nodes in Consent Acquisition Functionality in an immutable and non-repudiable manner;

(g) maintain with minimum performance requirements as specified;

(h) perform any other function and keep relevant details required for carrying out pre and post checks for regulatory compliance;

(3) Content Template Registrar (CTR) to

(a) carry out content template registration function;

(b) keep records of registered templates in immutable and non repudiable manner;

(c) maintain with minimum performance requirements as specified;

(d) perform any other function and keep relevant details required for carrying out pre and post checks for regulatory compliance;

(4) Content Format and Type Verifiers (CFTV) to

(a) carry out content verification;

(b) keep records with all relevant details for future references;

(5) Telemarketers for Scrubbing function (TM-SF) to

(a) carry out scrubbing;

(b) keep record of all numbers scrubbed for complaints resolution;

(c) maintain with minimum performance requirements as specified;

(d) perform any other function and keep relevant details required for carrying out pre and post checks for regulatory compliance;

(6) Telemarketers for Delivery Function of Messages with telecom resource connectivity to AP (TM-DF) to

(a) carry out delivery function

(b) insert its Unique identity with delivery processing reference number along with identity through which scrubbing was carried out;

(c) authenticate source of the messages submitted for delivery by header assignee or by aggregator and ensure their identity is part of content of message for traceability;

(d) maintain with minimum performance requirements as specified;

(e) perform any other function and keep other relevant details which may be required for carrying out pre and post checks for regulatory compliance;

(7) Telemarketers for Aggregation Function for messages to other Telemarketer for delivery function

IndiaCode

(TM-AF) to

(a) carry out aggregation function;

(b) keep record of all numbers aggregated for complaints resolution and traceability;

(c) authenticate source of the messages submitted for delivery by header assignee or by aggregator and ensure their identity is part of content of message for traceability;

(d) maintain with minimum performance requirements as specified;

(e) perform any other function and keep other relevant details which may be required for carrying out pre and post checks for regulatory compliance;

(8) Telemarketer for voice calling function with Telecom Resource Connectivity for voice calls to Access Provider (TM-VCF) to

(a) to carry out voice calling function;

(b) take necessary measures to protect Preference Register and Consent Register data during voice calling, e.g. using virtual identities to make voice calls on a secure Internet Protocol (IP) based Virtual Private Networks (VPN) with OAP and not disclosing real identities to any other entities than authorized to know it;

(c) take initiatives to enable calling name display (CNAM) based on Intelligent Network or ISDN based protocols, enhanced calling name (eCNAM) functionality as defined in 3GPP technical specifications TS 24.196 for providing services to terminating user with the name associated with the originating user and optionally delivering metadata about that originating user;

(d) maintain with minimum performance requirements as specified;

(e) perform any other function and keep other relevant details which may be required for carrying out pre and post checks for regulatory compliance;

6. Every Access Provider shall ensure that

(1) content of any commercial communication sent by the sender(s) shall be categorized and compared with the list of preference(s) of the recipient and/or purpose of consent given by the recipient to the sender for the purpose of scrubbing and for this purpose access provider shall ensure that

(a) any commercial communication through its network takes place only using registered content template(s) for transaction and/ or content template(s) for promotion;

(b) Unique Identity for registered template of content shall be assigned to the sender(s) at the time of registration of content template;

(c) Following Label shall be prefixed by the access provider to the text of commercial communication:

(i) *Label <Transactional> in case of Transactional Message;*

(ii) *Label <Service> in case of Service Message;*

(iii) *Label <Promotional> in case of Promotional Message;*

(d) Every Access Provider shall suffix relevant information required to revoke the consent to the text of promotional message;

(e) Content template shall be recorded on Distributed Ledger for Content Template (DL-CT) in an immutable and non repudiable manner;

(2) commercial communication is sent to the particular telephone number(s) in the target list of

IndiaCode

telephone numbers provided by the sender, to whom he wishes to send commercial communication only after scrubbing the target list and scrubbing includes

(a) verification of preference(s) by comparing the target telephone numbers, category of content with the list of telephone numbers and preference(s) of category of content by the target recipient customer in the Distributed Ledger for Preference (DL-Preference); and

(b) verification of consent(s) by comparing the target telephone number(s), category of content with the list of telephone numbers and consent(s) given by the recipient to the sender in the Distributed Ledger for Consent (DL-Consent); and

(c) verification of time band(s) by comparing the target telephone number(s), type of target time band for delivery with the list of telephone numbers and preference(s) of time band(s) of target recipient customer in Distributed Ledger for Preference (DL-Preference); and

(d) verification of type of day(s) by comparing the target telephone number(s), type of target day(s) for delivery with the list of telephone numbers and preference(s) of type of day(s) of target recipient customer in Distributed Ledger for Preference (DL-Preference);

(e) output of scrubbed list is a positive match of verifications in either of 2(a) or 2(b) as consent given by the recipient to the sender(s) shall override choice of preference(s) made by the recipient customer and positive match of verifications in 2(c) or 2(d);

7. Every Access Provider shall formulate: -

(1) Message Sequence Charts for messages with parameter details and time sequence to provide details about the process between two entities and action taken by particular entity;

(2) Flow Charts to provide details about the process between two entities and action taken;

IndiaCode

**SCHEDULE-II**

**Code of Practice for Process of registration, modification or deregistration of Preferences, recording consent and revocation of consent**

1. Procedure for registration or change of preference of Categories of content for Commercial Communications: -

(1) Customer can opt-out for any or all of following Commercial Communications Content category(ies) of content:

| ***Commercial Communications Category to be blocked or opted out*** | ***IVRS: Call to 1909 and press at prompt to block*** | ***SMS: Send SMS to 1909 following text*** | ***USSD: Dial USSD String*** |
|---|---|---|---|
| ***All CC Categories (to be blocked) except transactional type of commercial communications*** | ***0*** | *FULLY BLOCK* | *1909*0# |
| ***All CC Categories (to be blocked) except transactional and service type of commercial communications*** | ***50*** | *BLOCK PROMO* | *1909*50# |
| (i) *Banking/Insurance/Financial products/ credit cards,* | *1* | *BLOCK 1* | *1909*1# |
| (ii) *Real Estate,* | *2* | BLOCK 2 | *1909*2# |
| (iii) *Education,* | *3* | BLOCK 3 | *1909*3# |
| (iv) *Health,* | *4* | BLOCK 4 | *1909*4# |
| (v) *Consumer goods and automobiles,* | *5* | BLOCK 5 | *1909*5# |
| (vi) *Communication/Broadcasting / Entertainment/IT,* | *6* | BLOCK 6 | *1909*6# |
| (vii) *Tourism and Leisure,* | *7* | BLOCK 7 | *1909*7# |
| (viii) *Food and Beverages;* | *8* | BLOCK 8 | *1909*8# |

IndiaCode

*Note-1: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-out may be communicated;*

*Note-2: Customer to be communicated with confirmation and final status along with options to unblock;*

*Note-3: FULLY BLOCK option shall put the customer in Fully Blocked state and block service as well as promotional types of commercial communications for all categories of content, mode, time band and day types;*

*Note-4: BLOCK PROMO option shall block only promotional types of commercial communications for all categories of content, mode, time band and day types except service and transaction type of commercial communications;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub

category(ies) for content;

(2) Customer can opt-in for any or all of following Commercial Communications Content category(ies) of content:

| ***UCC Category to be unblocked or opted in*** | ***IVRS: Call to 1909 and press at prompt to unblock*** | ***SMS to 1909 following text*** | ***USSD send*** |
|---|---|---|---|
| ***All UCC Categories (to be unblocked)*** | ***90*** | *UNBLOCK ALL* | *#1909*90# |
| ***All UCC Categories (to be unblocked) except Promotional*** | ***51*** | *UNBLOCK SERVICE* | *#1909*51# |
| (i) *Banking/Insurance /Financial products/ credit cards,* | *91* | *UNBLOCK 91* | *#1909*91# |
| (ii) *Real Estate,* | *92* | UNBLOCK 92 | *#1909*92# |
| (iii) *Education,* | *93* | UNBLOCK 93 | *#1909*93# |
| (iv) *Health,* | *94* | UNBLOCK 94 | *#1909*94# |
| (v) *Consumer goods and automobiles,* | *95* | UNBLOCK 95 | *#1909*95# |
| (vi) *Communication/Broadcasting/ Entertainment/IT,* | *96* | UNBLOCK 96 | *#1909*96# |
| (vii) *Tourism and Leisure,* | *97* | UNBLOCK 97 | *#1909*97# |
| (viii) *Food and Beverages;* | *98* | UNBLOCK 98 | *#1909*98# |

IndiaCode

*Note-1: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-in may be communicated;*

*Note-2: Customer to be communicated with confirmation and final status along with options to block*

*Note-3: UNBLOCK ALL option shall unblock all categories of content, mode, time band and day types with default options;*

*Note-4: UNBLOCK 51 shall restore service type of commercial communications for all categories of content, mode, time band and day types as per the previous state of the customer while he exercised block option last time or with the default options as the case may be while promotional type of commercial communications shall remain in blocked state;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for content;

2. Procedure for registration of preference or change of preference of Mode for Commercial

Communications: -

(1) Customer can opt-out of any or all of following category(ies) of mode(s) of communication:

| ***UCC Mode of Communication (Choices for Preference(s))*** | ***IVRS: Call to 1909 and press at prompt to block*** | ***SMS: Send SMS to 1909 following text*** | ***USSD: Dial USSD String*** |
|---|---|---|---|
| ***All Categories of Mode (to be blocked)*** | ***10*** | *BLOCK 10* | *1909*10# |
| (i) *Voice Call,* | *11* | *BLOCK 11* | *1909*11# |
| (ii) *SMS,* | *12* | BLOCK 12 | *1909*12# |
| (iii) *Auto Dialer Call (With Pre-recorded Announcement),* | *13* | BLOCK 13 | *1909*13# |
| (iv) *Auto Dialer Call (With Connectivity to live agent),* | *14* | BLOCK 14 | *1909*14# |
| (v) *Robo-Calls,* | *15* | BLOCK 15 | *1909*15# |

IndiaCode

*Note-1: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-out may be communicated;*

*Note-2: Customer to be communicated with confirmation and final status along with options to unblock;*

*Note-3: BLOCK 10 option shall block all categories of modes except transactional type commercial communications while saving the status of customer for categories of time band and day types;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for mode;

(2) Customer can opt-in for any or all of following category(ies) of mode(s) of communication:

| ***UCC Mode of Communication (Choices for Preference(s))*** | ***IVRS: Call to 1909 and press at prompt to block*** | ***SMS: Send SMS to 1909 following text*** | ***USSD: Dial USSD String*** |
|---|---|---|---|
| ***All Categories of Mode (to be unblocked)*** | ***80*** | *UNBLOCK 80* | *1909*80# |
| (i) *Voice Call,* | *81* | *UNBLOCK 81* | *1909*81# |
| (ii) *SMS,* | *82* | UNBLOCK 82 | *1909*82# |
| (iii) *Auto Dialer Call (With Pre-recorded Announcement),* | *83* | UNBLOCK 83 | *1909*83# |
| (iv) *Auto Dialer Call (With Connectivity to live agent),* | *84* | UNBLOCK 84 | *1909*84# |
| (v) *Robo-Calls,* | *85* | UNBLOCK 85 | *1909*85# |

*Note-1: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-in may be communicated;*

*Note-2: Customer to be communicated with confirmation and final status along with options to block;*

*Note-3: UNBLOCK 80 option shall restore all categories of modes for categories of time band and day types as per the previous status of customer when he exercised block option last time or as per the default options as the case maybe;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for modes;

3. Procedure for registration or change of preference of Time band(s) for Commercial Communications: -

(1) Customer can opt-out of any or all of following time bands for receiving of commercial communications:

| ***UCC Time band for Communication (Choices for Preference(s))*** | ***IVRS: Call to 1909 and press at prompt to block*** | ***SMS: Send SMS to 1909 following text*** | ***USSD: Dial USSD String*** |
|---|---|---|---|
| ***All Time Bands (to be blocked)*** | ***20*** | *BLOCK 20* | *1909*20# |
| (i) *00:00 Hrs to 06:00 Hrs,* | *21* | *BLOCK 21* | *1909*11# |
| (ii) *06:00 Hrs to 08:00 Hrs,* | *22* | BLOCK 22 | *1909*22# |
| (iii) *08:00 Hrs to 10:00 Hrs,* | *23* | BLOCK 23 | *1909*23# |
| (iv) *10:00 Hrs to 12:00 Hrs,* | *24* | BLOCK 24 | *1909*24# |
| (v) *12:00 Hrs to 14:00 Hrs,* | *25* | BLOCK 25 | *1909*25# |
| (vi) *14:00 Hrs to 16:00 Hrs,* | ***26*** | BLOCK 26 | *1909*26# |
| (vii) *16:00 Hrs to 18:00 Hrs,* | *27* | BLOCK 27 | *1909*27# |
| (viii) *18:00 Hrs to 21:00 Hrs,* | *28* | BLOCK 28 | *1909*28# |
| (ix) *21:00 Hrs to 24:00 Hrs,* | *29* | BLOCK 29 | *1909*29# |

IndiaCode

*Note-1: Time Bands (i), (ii), (iii) and (ix) shall be default OFF for all customers irrespective of the status of registration of customer i.e. for all customers including those who have not registered any type of preference(s), anytime unless customer has registered its preference(s) and switched ON;*

*Note-2: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-out may be communicated;*

*Note-3: Customer to be communicated with confirmation and final status along with options to unblock;*

*Note-4: BLOCK 20 option shall block all categories of modes while saving current status of customer for categories of content, time band and day types, however transactional type of commercial communications may not be blocked;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for time band;

(2) Customer can opt-in for any or all of following time band(s):

| ***UCC Time band for*** | ***IVRS: Call to 1909*** | ***SMS: Send SMS to*** | ***USSD: Dial*** |
|---|---|---|---|

| ***Communication (Choices for Preference(s))*** | ***and press at prompt to block*** | ***1909 following text*** | ***USSD String*** |
|---|---|---|---|
| ***All Time Bands (to be unblocked)*** | ***70*** | *UNBLOCK 70* | *1909*70# |
| (i) *00:00 Hrs to 06:00 Hrs,* | *71* | *UNBLOCK 71* | *1909*71# |
| (ii) *06:00 Hrs to 08:00 Hrs,* | *72* | UNBLOCK 72 | *1909*72# |
| (iii) *08:00 Hrs to 10:00 Hrs,* | *73* | UNBLOCK 73 | *1909*73# |
| (iv) *10:00 Hrs to 12:00 Hrs,* | *74* | UNBLOCK 74 | *1909*74# |
| (v) *12:00 Hrs to 14:00 Hrs,* | *75* | UNBLOCK 75 | *1909*75# |
| (vi) *14:00 Hrs to 16:00 Hrs,* | ***76*** | UNBLOCK 76 | *1909*76# |
| (vii) *16:00 Hrs to 18:00 Hrs,* | *77* | UNBLOCK 77 | *1909*77# |
| (viii) *18:00 Hrs to 21:00 Hrs,* | *78* | UNBLOCK 78 | *1909*78# |
| (ix) *21:00 Hrs to 24:00 Hrs,* | *79* | UNBLOCK 79 | *1909*79# |

*Note-1: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-out may be communicated;*

*Note-2: Customer to be communicated with confirmation and final status along with options to block;*

*Note-3: UNBLOCK 70 shall restore all categories of time bands for the customer in which he was before he exercised option to block last time, if any, otherwise as per the default options;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for time band;

4. Procedure for registration or change of preference of Day Type(s) for Commercial Communications: -

(1) Customer can opt-out of any or all of following day type(s):

| ***UCC Day Type(s) for receiving Communication (Choices for Preference(s))*** | ***IVRS: Call to 1909 and press at prompt to block*** | ***SMS: Send SMS to 1909 following text*** | ***USSD: Dial USSD String*** |
|---|---|---|---|
| ***All Day Type(s) (to be blocked)*** | ***30*** | *BLOCK 30* | *1909*30# |
| (i) *Monday* | *31* | *BLOCK 31* | *1909*31# |
| (ii) *Tuesday* | *32* | BLOCK 32 | *1909*32# |
| (iii) *Wednesday* | *33* | BLOCK 33 | *1909*33# |
| (iv) *Thursday* | *34* | BLOCK 34 | *1909*34# |
| (v) *Friday* | *35* | BLOCK 35 | *1909*35# |
| (vi) *Saturday* | *36* | BLOCK 36 | *1909*36# |

IndiaCode

| | | | |
|---|---|---|---|
| (vii) *Sunday* | *37* | BLOCK 37 | *1909*37# |
| (viii) *Public Holiday and National Holiday* | *38* | BLOCK 38 | *1909*38# |

*Note-1: Time Bands (i), (ii), (iii) and (ix) shall be default OFF for all customers irrespective of the status of registration of customer i.e. for all customers including those who have not registered any type of preference(s), anytime unless customer has registered its preference(s) and switched ON;*

*Note-2: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-in may be communicated;*

*Note-3: Customer to be communicated with confirmation and final status along with options to unblock;*

*Note-4: BLOCK 30 option shall block all categories of types of days while saving the status of customer for categories of time band and day types, however transactional type of commercial communications may not be blocked;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for day type(s);

(2) Customer can opt-in for any or all of following day type(s):

| ***Day Type(s) for receiving Commercial Communication (Choices for Preference(s))*** | ***IVRS: Call to 1909 and press at prompt to block*** | ***SMS: Send SMS to 1909 following text*** | ***USSD: Dial USSD String*** |
|---|---|---|---|
| ***All Day Type(s) (to be unblocked)*** | ***60*** | *UNBLOCK 60* | *1909*60# |
| (i) *Monday* | *61* | *UNBLOCK 61* | *1909*61# |
| (ii) *Tuesday* | *62* | UNBLOCK 62 | *1909*62# |
| (iii) *Wednesday* | *63* | UNBLOCK 63 | *1909*63# |
| (iv) *Thursday* | *64* | UNBLOCK 64 | *1909*64# |
| (v) *Friday* | *65* | UNBLOCK 65 | *1909*65# |
| (vi) *Saturday* | ***66*** | UNBLOCK 66 | *1909*66# |
| (vii) *Sunday* | *67* | UNBLOCK 67 | *1909*67# |
| (viii) *Public Holiday and National Holiday* | *68* | UNBLOCK 68 | *1909*68# |

*Note-1: In case of communication with customer executive of Customer Care Center of access provider, preference to opt-in may be communicated;*

*Note-2: Customer to be communicated with confirmation and final status along with options to block;*

*Note-3: UNBLOCK 60 shall restore all categories of types of day for the customer in which he was before he exercised option to block last time, if any, otherwise as per the default options;*

*Provided* that the Authority may, from time to time, add or remove number of category(ies), or sub category(ies) for day type(s);

IndiaCode

5. Recording preferences on Distributed Ledger for Preferences (DL-Preferences)

(1) Access Provider shall automate its internal systems and develop appropriate APIs to interact with DL-Preferences;

(2) Access Provider shall record preferences on DL-Preferences within 15 minutes for requests received from all modes;

(3) These revised preferences shall be available, in real time, for considerations by entities for scrubbing process for new list of telephone numbers under process, however, earlier messages or voice calls which have already been scrubbed and have validity may be delivered;

6. Every Access Provider shall establish, maintain and operate Distributed Ledger(s) for Preference (DL-Preference) with requisite functions, process and interfaces: -

(1) to record choices of preference(s) exercised by the customer in the Distribute Ledger for Preferences (DL-Preferences) in an immutable and non repudiable manner;

(2) to record, at least, following details of the customer who has registered its preference(s):

(a) telephone number in the international numbering format as referred in the National Numbering Plan;

(b) Location Routing Number (LRN), as assigned by DoT to the access provider, of current serving network of the customer and changes in LRN of the new serving network, in case customer is being ported-in during Mobile Number Portability;

(c) lifetime history, with date(s) and time stamp(s), of choices exercised by the customer for registering his preference(s) and subsequent changes to it made by the customer from time to time;

(d) changes in the subscription of telephone number, during the process of opening and closing of subscription;

(e) unique registration number issued at the time of registration of preference(s);

(3) to interact and exchange information with other relevant entities, responsible to carry out functions for regulatory compliance(s), in a safe and secure manner;

(4) to support any other functionalities as may be required to carry out functions for regulatory compliance(s);

7. Every Access Provider shall establish facility for revoking the consent by its customers and shall make necessary arrangements: -

(1) to receive request, from the customer, for revoking the consent, if any, given by the recipient to the sender or to the consent acquirer for the purpose of receiving a commercial communication message or voice call;

(2) to provide modes, free of cost, to the customer, as per his choice, to revoke consent either by: -

*(i) sending SMS to short code 1909 with Label <Revoke> and <Sender ID> or to telephone number mentioned in the message or during the voice call received from the sender(s); or*

*(ii) calling on 1909 or number mentioned for revoking the consent during the voice call received from the sender(s); or*

*(iii) calling on customer care number; or*

*(iv) Interactive Voice Response System (IVRS); or*

*(v) Mobile app developed in this regard either by the Authority or by any other person or entity and*

IndiaCode

*approved by the Authority; or*

*(vi) Web portal with authentication through OTP; or*

*(vii) Any other means as may be notified by the Authority from time to time.*

(3) to remove the recipient's contact information (telephone number to which the message was sent) from the consent record(s) corresponding to the sender for all purposes requiring explicit consent except in case specific purpose(s) is indicated by the customer during revocation of consent from the consent register within 1 business day;

(4) to duly acknowledge the customer's request to revoke the consent with unique reference number;

(5) to ensure that any person who receives request to revoke consent must not disclose the customer's personal information to others without his consent;

(6) to fetch details of the consent including its purpose(s), details about day and time when it was taken, and details about sender(s) or consent acquirer(s) who has or have taken the consent;

8. Every Access Provider shall establish, maintain and operate Distributed Ledger(s) for Consent (DL-Consent) with requisite functions, process and interfaces: -

(1) to record consent given by the customer to sender(s) or consent acquirer(s) in the Distribute Ledger for Consent (DL-Consent) in an immutable and non repudiable manner;

(2) to record, at least, following details of the consent: -

(a) telephone number of customer in international numbering format as referred in National Numbering Plan;

(b) Header of Sender(s) or Consent Acquirer(s) against which consent is taken;

(c) Day & Time when consent was taken;

(d) Validity period of consent;

(e) Type and purpose(s) of consent;

(3) to make consent data accessible for other entities in safe and secure manner;

(4) to keep record of revocation of consent by the customer with specific purpose(s), if any, in an immutable and non-repudiable manner;

(5) to interact and exchange information with other relevant entities, responsible to carry out functions for regulatory compliance(s), in a safe and secure manner;

(6) to support any other functionalities as may be required to carry out functions for regulatory compliance(s);

9. Every Access Provider shall specify: -

(1) Entity and process for generation of One Time Password (OTP) for different purposes and its validity period;

(2) Entity and process for verification of OTP received from the customer or for verification of entity carrying out activity under Code(s) of Practice for Entities;

10. Every Access Provider shall formulate: -

(1) Message Sequence Charts for messages with parameter details and time sequence to provide details about the process between two entities and action taken by particular entity;

IndiaCode

(2) Flow Charts to provide details about the process between two entities and action taken;

IndiaCode

**SCHEDULE-III**

**List of Action items for Code of Practice for Complaint Handling (CoP-Complaints)**

1. Every Access Provider shall formulate Code of Practice for Complaint handling (CoP-Complaints) and shall prescribe role, responsibilities of entities involved in examining, investigating and resolving complaints;

2. CoP-Complaints shall also include details about: -

   (1) Complaint registration through voice call

   (a) Procedure for a customer to make a call to 1909 for registering his complaint.

   (b) Procedure and role of the customer care executive to interact with the customer about the details like particulars of telemarketer, the telephone number from which the unsolicited commercial communication has originated the date, time and brief description of such unsolicited commercial communication.

   (c) Procedure and role of the customer care executive to register the customer complaint and acknowledge the complaint by providing a unique complaint number.

   (2) Complaint Registration through SMS

   (a) Format for making complaints in which a customer may register his complaint pertaining to receipt of unsolicited commercial communication.

   (b) Details to be provided by the complainant e.g. Unsolicited Commercial Communications with date on which it was received along with content of received message and in case of voice call, brief of content of communication etc.

   (3) Complaint registration through a mobile app

   (a) Functioning of intelligent and intuitive mobile app(s) for devices with different operating systems and helping customer to identify and report suspected sources of spam and also making use of it by the customer to make complaints;

   (b) Ways and means which can be used to enhance mobile App and other modes for the customer to help him to identify probable source of spam in an intelligent manner and offers to select source of messages and voice calls against which complaint is to be made;

   (c) Ways and means which can be used by the customer to compose complaint on behalf of recipient in a convenient manner and quickly;

   (d) App which helps user of app to keep track of complaints made earlier for the app user;

   (e) Ways and means to Increase adoption of App to quickly detect spam participate to actively report to lead to larger set of information helpful to curb menace of Unsolicited Commercial Communications;

   (4) Complaint registration through Web Portal

   (a) Procedure for the customer to make complaints by visiting website of access provider and register his complaint.

   (b) Procedure for filling form and design it for the purpose of filing complaint with all relevant details required to investigate complaint and take appropriate action;

   (c) Procedure for authentication process to ensure that complaint is made by recipient;

   (d) Procedure to generate and communicate Reference number to the customer which may be used

IndiaCode

to check status of complaint;

3. Every Access Provider shall formulate: -

(1) Message Sequence Charts for messages with parameter details and time sequence to provide details about the process between two entities and action taken by particular entity;

(2) Flow Charts to provide details about the process between two entities and action taken;

IndiaCode

**Schedule-IV**

**Action Items for preparing Code of Practice for Unsolicited Commercial Communications Detection (CoP-UCC_Detect)**

1. Every Access Provider shall establish, maintain and operate following system, functions and processes to detect sender(s) who are sending Unsolicited Commercial Communications in bulk and not complying with the regulation(s), and act to curb such activities: -

   (1) System which have intelligence at least following functionalities: -

   (a) identifying sender(s) on basis of signature(s);

   (b) deploying honeypot(s) and using information collected by it;

   (c) evolving signature(s) by learning over time;

   (d) interface to exchange information with similar system(s) established by other access provider(s) to evolve signature(s), detecting sender using Sender Information (SI);

   (e) considering inputs available from DL-Complaints about complaints and reports and analyze them;

   (f) considering inputs available, if any, from any other network element(s) of the access provider system(s);

   (2) provide ways and means for resolving complaint(s) by sharing information related to telephone number(s) of sender(s) against which complaint is made;

2. Every Access Provider shall formulate codes of practice (CoP-UCC_Detect) for system, functions and process prescribed as following: -

   (1) implementation details for detecting Unsolicited Commercial Communications related to suspicious unregistered telemarketing activity using Signature solution, deploying honeypots and other technical measures;

   (2) minimum standards of technical measures to share intelligence information, rules, criteria to detect suspected sources of spam;

   (3) approaches to detect and identify unregistered Unsolicited Commercial Communications sender(s), who are camouflaging themselves by fragmenting their activity across multiple phone numbers;

   (4) approaches for deployment of honeypots to capture Unsolicited Commercial Communications voice call(s);

   (5) approaches to detect and identify source(s) of dictionary attacks;

   (6) timeline(s) for implementation of the functionality referred in code of practice and operationalizing it;

   (7) such other matters as the Authority may deem fit, from time to time.

3. Report of entities found to be engaged in making or causing to make silent calls, robocalls, abandoned calls or using telephone directory harvesting software to make Unsolicited Commercial Communications, as and when came to notice of the access provider, or as provided for in the regulations for the registered sender(s) with the access providers, on basis of following criteria: -

   (a) Ratio of Abandon Calls to total attempted calls for a registered entity exceeding 3% over a period of 24 Hours by an entity using Auto Dialer for Commercial Communications calls;

   (b) Ratio of Silent Calls to total attempted calls for a registered entity exceeding 1% over a period of 24

IndiaCode

hour by an entity using Auto Dialer for Commercial Communications Calls;

(c) Entity(ies) found to be using telephone number harvesting software for sending Unsolicited Commercial Communications are barred to use their network;

IndiaCode

**Schedule-V**

**Action Items for preparing Code of Practice for Periodic Monthly Reporting (CoP-PMR)**

1. Maintaining records of complaints on daily basis for each service area: -

   (a) total number of complaints received on each day, from its customers as Terminating Access Provider, in each service area, against any registered sender;

   (b) total number of complaints transferred on each day, to Originating Access Provider(s) including itself, in each service area, against any registered sender;

   (c) total number of complaints to be resolved as an Originating Access Provider, according to the date of receipt of complaints;

   (d) total number of complaints rejected on account of insufficient details for further examination, according to the date of receipt of complaint;

   (e) total number of complaints to be resolved as an Originating Access Provider, according to the date of occurrence of unsolicited commercial communication;

   (f) total number of senders against whom complaints were reported under clause (c);

   (g) total number of complaints out of reported complaints under clause (f), after completion of investigation, found to be valid complaint(s);

   (h) total number of senders out of reported senders under clause (f), found to be non-compliant as per the provisions provided for in these regulations or Code(s) of Practice;

   (i) total number of senders out of reported senders under clause (h), who were put under restricted limits of usage provided for in Code(s) of Practice, as an interim measure to control unsolicited commercial communications during the investigation phase;

   (j) numbers of commercial communications sent by each sender, reported under clause(i);

   (k) total number of entities other than sender(s), after completion of investigation, found to be not compliant to the provisions provided for in these regulations or Code(s) of Practice and actions taken against them;

   (l) report total number of complaints on a day, for any sender, reported under clause(h);

2. Maintain records of complaints, from its customers and received from Terminating Access Provider(s), against unregistered sender(s) for sending unsolicited commercial communications on daily basis for each service area: -

   (a) total number of complaints received on each day, from its customers as Terminating Access Provider, in each service area, against any unregistered sender;

   (b) total number of complaints transferred on each day, to Originating Access Provider(s) including itself, in each service area, against any unregistered sender;

   (c) total number of complaints to be resolved as an Originating Access Provider, according to the date of receipt of complaints;

   (d) total number of complaints rejected on account of insufficient details for further examination, according to the date of receipt of complaint;

   (e) total number of complaints to be resolved as an Originating Access Provider, according to the date of occurrence of unsolicited commercial communication;

(f) total number of senders against whom complaints were reported under clause (e);

(g) total number of complaints out of reported complaints under clause(e), after completion of investigation, found to be valid complaint(s);

(h) total number of senders, under clause(f) against whom complaints were found to be valid;

(i) total number of senders out of reported senders under clause(h), who were put under usage cap, as an interim measure to control unsolicited commercial communications during the investigation phase;

(j) total number of senders out of reported senders under clause (i), who were put under Usage Cap or disconnected, after conclusion of the investigation with following breakup: -

(i) *number of senders who were given warning against first instance of violations;*

(ii) *number of senders found to violating second time;*

(iii) *number of senders found to be violating third or more number of times;*

(k) numbers of commercial communications sent by each sender, reported under clause(h);

(l) total number of outgoing communications made by the sender(s), reported under clause(f) and exceeding the restriction limits from the deemed date of imposition of such restrictions;

IndiaCode

**Schedule-VI**

**List of key activities (but not an exhaustive list) for preparation of migration plan**

(1) Introducing Distributed Ledger (DL) for registration of entities (DL-Entities);

(a) To register entities declared by access provider or access provider(s) together for various functions and registers like

(i) *Header Register;*

(ii) *Consent Register;*

(iii) *Consent Template Register;*

(iv) *Content Template Register;*

(v) *Content Template Verifier;*

(vi) *Complaint Register;*

(vii) *Preference Register;*

(viii) *Telemarketer Scrubbing Function Register;*

(ix) *Telemarketer Message Delivery Function Register;*

(x) *Telemarketer Voice Delivery Function Register;*

(b) Deadline(s) for registering entities with DL-Entities

(i) *Header Register;*

(ii) *Consent Register;*

(iii) *Consent Template Register;*

(iv) *Content Template Register;*

(v) *Content Template Verifier;*

(vi) *Complaint Register;*

(vii) *Preference Register;*

(viii) *At least one entity for Telemarketer Scrubbing Function;*

(ix) *At least one entity for Telemarketer Message Delivery Function Register;*

(x) *At least one entity for Telemarketer Voice Delivery Function Register;*

(2) Registration of existing assignee of Headers with Header Registrar;

(a) stop assigning headers without verification of identity and scope of senders;

(b) register existing assignee of headers after verification of identity and scope documents of Unsolicited Commercial Communications sender(s) and bind to phone number(s);

(c) assign or reassign current owner of header(s) considering at least following: -

(i) *Whether headeris not assigned to any other sender(s);*

(ii) *Whether header is matching with brand name of a company;*

(iii) *Whether header is look alike with other popular header(s) and may mislead recipients;*

(iv) *Any other reason or fact which is important to consider before assigning header;*

(d) use temporary header(s), during migration phase, for all earlier assigned headers;

(e) fixing deadline for working of temporary headers;

IndiaCode

(3) Start assigning new headers

(a) assign headers after due diligence, verification of identity and scope documents of Unsolicited Commercial Communications sender(s) and bind to phone number(s);

(b) consider reason(s) and fact(s) which are important to be considered before assigning headers and do not mislead recipients;

(c) consider headers which may be required to be reserved for central and state government entities and also for statutory bodies;

(4) Develop mobile app for devices which may be required for senders during login to sessions for various activities like scrubbing, submission of messages to delivery, making voice calls etc.;

(5) Introduce telemarketer with scrubbing function, separate from telemarketer with delivery function

(6) Scrubbing envisaged in final form to be achieved in phased manner

(i) *Initially, using data from existing register for customers' preferences;*

(ii) *subsequently, using records of DL-Preferences;*

(iii) *then using records of DL for Header Register;*

(iv) *then introducing virtual identities and tokens among entities to access real identities;*

(v) *then using records of DL for consent;*

(7) Introduce DL for Complaints;

(8) Register existing consents on Consent Register;

(a) Register existing consents with consent registrar in robust manner to make it non-repudiable;

(b) stop taking consent not in accordance to these regulations;

(c) fix deadline for expiry of consent not registered with consent registrar;

(9) Register new consents on consent register as prescribed in relevant regulations or schedule or directions

(a) Develop Application Programme Interfaces (APIs) for Senders to recording consent with user agent or application client available on a mobile device or enterprise system;

(b) Broadening of installation and active base of consent acquisition application client;

(10) Make consent system ready to become part of scrubbing for all cases;

(11) Migration of existing registers with TRAI;

(a) Migrate NCPR data to DL-Preferences and have observer node for TRAI;

(b) Migrate Telemarketer registration module data of National Telemarketer Register (NTR) to DL-Entities and have observer node for TRAI;

(c) Migrate complaint module data to DL-Complaints and have observer node for TRAI;

(12) Introduce observer node of DL-Consents and observer nodes of rest of registers envisaged in the relevant regulations;

(13) Enhance signature solution capabilities and exchange intelligence information, rule, criteria and other relevant information among access providers to detect and identify suspicious Unregistered Telemarketing Activities more effectively and efficiently;

IndiaCode

(14) Deploy honeypots to detect and identify suspicious Unsolicited Commercial Communications Voice calls by capturing relevant information;

IndiaCode

## Explanatory Memorandum

# 1 Introduction

## 1.1 Overview

1.1.1 Unsolicited Commercial Communications (UCC) are communications, made via voice calls or SMS, to subscribers without their consent or willingness. Apart from being a source of inconvenience, such communications also impinge on the privacy of individuals.

1.1.2 To curb UCC, the Telecom Regulatory Authority of India (TRAI) notified the Telecom Unsolicited Commercial Communications Regulations (TUCCR), 2007 dated 5th June 2007, which put in place a framework for controlling UCC. These regulations were reviewed in year 2010 and TRAI released new regulations known as Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2010) which were notified on 1st December 2010. Summary of these regulations, amendments made over a period and directions issued are given in sub-paras 1.2 to 1.4.

1.1.3 Despite taking various measures, UCC related complaints are on the rise and the problem is not fully under control. Therefore, TRAI initiated consultation process on 14th of September 2017 to seek inputs from stakeholders on how to overcome the problems and plug loopholes in the system. Main heading 2 summarizes the issues and give a brief about the consultation process.

1.1.4 For sake of convenience, issues related to system of Registration of Related Entities (including Consents given by the customer to senders) are deliberated upon first, as they deal with the UCC eco system to govern commercial communication from registered entities. It is the part where changes in regulatory approach are the most important and technology driven solutions play an important role. Next, the system for Customer Preference Registration is deliberated upon, which can leverage capabilities introduced in the UCC eco system; followed by the system for Complaint Handling or redressal. Finally, the technology to be adopted for core network of UCC eco systems is discussed, with details about its capabilities and usefulness in the context of UCC.

1.1.5 Main heading 3, 4 and 5 provide summary of issues related to entities of UCC eco system, Customer Preference Registration System and Complaint Handling System respectively. These Paras also summarize the comments of stakeholders on the issues, analysis of inputs and decisions of the Authority.

1.1.6 Main heading 6 to 10 analyze Distributed Ledger Technology (DLT) from perspective of regulatory compliance through adoption of the technology. It provides details of capabilities of DLT, its important properties, types of DLT networks and summarizes appropriateness of type of DLT network for UCC eco system.

1.1.7 Finally, main heading 11 summarizes impact of new regulations on access providers and eco system. It also summarizes benefits of implementing new regulations to different stakeholders.

## 1.2 Regulatory Framework notified in 2007

1.2.1 These regulations envisaged the establishment of a National Do Not Call (NDNC) Registry to facilitate registration of requests from customers who do not wish to receive UCC. To improve the effectiveness of the framework, the Authority subsequently amended these regulations, incorporated financial disincentives for non-compliance with regulatory provisions by the telecom service providers. These regulations were further amended to simplify the customer enrolment process, smoothening the system for redressal of complaints related to UCC and imposing financial disincentives on Access Providers for non-compliance with regulatory provisions.

1.2.2 Despite measures taken by the Authority for curbing Unsolicited Commercial Communications,

dissatisfaction among telecom customers continued on this account and the regulatory framework set up by TUCCR-2007 was found to be not effective and it needed revision.

1.2.3 The major issues impacting the effectiveness of the TUCCR-2007 regulations were privacy, the lengthy and unfriendly procedure for registration of telemarketers that could discourage telemarketers from registration, difficulty in scrubbing the NDNC data by telemarketers, lack of stringent penal provisions, etc. In the year 2010, TRAI initiated a consultation process to review TUCCR-2007. On the basis of consultation done, Authority notified revised regulatory framework on 1st December 2010, as Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2010).

### 1.3 Revised Regulatory Framework notified in 2010

1.3.1 TCCCPR-2010 notified on 1st of December 2010 came into effect in a phased manner and were amended several times. Regulations 1 to 2 and 23 to 25 came into force on the date of notification, while a few (13 to 17) were supposed to come into effect on 15th Dec. 2010 and rest (3 to 12 and 18 to 22) were supposed to come into effect on 1st Jan. 2011. Dates of enforcement of some of these regulations were revised due to implementation issues, and with revised dates, all regulations came into force by 27th of November 2011. The key regulatory requirements in this framework were:

i. *Mandatory registration of telemarketers with TRAI after payment of a one-time fee of Rs. 10,000/-*

ii. *Enabling consumers to block receiving of promotional messages by registering the number in the National Preference Register (NCPR)*

iii. *Requiring telemarketers not to send messages to those customers who specifically choose not to receive such messages by registering in NCPR; and*

iv. *Deduction from the security deposit of registered telemarketers who breach the provisions of the regulations by sending commercial messages to the customers registered in NCPR.*

IndiaCode

1.3.2 Aforesaid provisions were made in the regulations with the aim that if all telemarketers registered themselves with the Authority and the consumers electing not to receive promotional commercial messages register themselves in NCPR, the menace of UCCs would be controlled. Though some did register as telemarketers, many others chose to continue operating as telemarketers without registering themselves as such. They obtained multiple SIMs as "normal subscribers" and made calls or sent out messages (SMS) in bulk as UCCs to other telecom subscribers. To deal with the situations, and make regulations more effective, several amendments were made to the main regulations.

### 1.4 Amendments to Main Regulations of 2010 and Directions

1.4.1 To make regulations more effective and consider practical requirements of business and customers, these regulations have been amended time to time, some of important changes are:

| S.N. | Amendment to TCCCPR 2010 | Key points |
|---|---|---|
| 1 | *1st Amendment*<br>*Dated 14th December 2010* | **Re-determination of dates** for implementation of regulations & sub-regulations due to the requirements of security audit of Website and process for the purpose of these regulations. |
| 2 | *2nd Amendment*<br>*Dated 28th December 2010* | **Re-determination of dates** for Regulations 3 to 12, 13 to 17 and 18 to 22. |

| | | |
|---|---|---|
| 3 | *3rd Amendment*<br>*Dated.31st January 2011* | **Re-determination of dates** for Regulations 3 to 11, 12 and 18 to 22 as time required for configuration changes and testing due to changes in level earmarked for telemarketing purposes from level '70' to level '140' for mobile networks. Overlapping period of regulations required timelines for withdrawing telecom resources already allotted to a telemarketer. |
| 4 | *4th Amendment*<br>*Dated 28th February 2011* | **Re-determination of dates** for Regulations 12, 17 and 18 to 22, due to high traffic volume for call centres and resources for Call Centers could not be met by mobile network alone and required allocation of level series for fixed network. More time required for implementation to carry out configuration and testing. |
| 5 | *5th Amendment*<br>*Dated 18th March 2011* | **Re-determination of dates** for Regulations 12, 17 and 18 to 22, due to non-availability of level series for telemarketers for fixed line networks. |
| 6 | *6th Amendment*<br>*Dated 5th September 2011* | **Re-determination of dates** for Regulations 12, 17 and 18 to 22 as Level '140' series allocated for telemarketers for fixed network on 16th August 2011.<br>**Added: "Transaction Message" definition**- information pertaining to Depositories registered with SEBI, DTH operators and information from a registered educational institution to its students.<br>**Added: Exempting Government and Statutory Bodies from definition of UCC**- any message transmitted by or on directions of bodies established under the Constitution or the Central Government or State Government, or the Authority or by any agency authorized by the Authority was exempted from the definition of UCC.<br>**Modified**: **Reduced time period to change preference-** for changing preferences reduced from three months to seven days.<br>**Introduced: timing restrictions for delivery of commercial communications-** commercial communication other than Transactional message to be sent only between 0900 to 2100 hrs.<br>**Added: Capping on SMS/ Day-** 100 (for pre-paid) and 300 SMS/SIM/Day (for post-paid) with provisions for exempting categories as specified from time to time.<br>**Introduced: Format and structure for SMS Header** in Schedule-I<br>'140' series and SMS headers for providing Telecom resources to Telemarketer for voice calls in Schedule-III |
| 7 | *7th Amendment*<br>*Dated 25th October 2011* | **Introduced: "Promotional SMS Charge"** as charge payable by an OAP to the TAP for each promotional SMS sent by a RTM from the network of the OAP to the network of TAP.<br>**Introduced: Transactional message directly by entity or through RTM-**Regulation 16-A added and modified relevant |

indiacode

| | | |
|---|---|---|
| | | regulations to include Transactional Messages Sending Entity (TMSE)<br><br>**Introduced: Provisions to not to offer concessional packages for SMS** (beyond a limit)<br><br>In sub-regulation 2 of regulation 20 added: no Access Provider to offer, other than an RTM or an entity sending transactional messages (TMSE), any tariff plan or SMS package permitting more than 100 SMS/ day/SIM except on 'blackout days'.<br><br>**Added:** OAP may collect **Promotional SMS charge Rs. 0.05** (five paisa only) from RTM (Regulation 20-A)<br><br>**Added:** Transactional Message Sending Entity in Schedule-V<br>**Modified: Complaint Format** in Schedule-VI (Procedure for registration of complaint) from comma to semi-colon as a separator in the complaint format to be submitted via SMS. |
| 8 | *8th Amendment*<br><br>*Dated 1st November 2011* | **Modified Capping on SMS/day**: In 20(2), Capping on maximum SMS allowed per day/SIM changed from 100 to 200 and another capping of 3000 SMS/month changed to 6000 SMS/month. |
| 9 | *9th Amendment*<br><br>*Dated 14th May 2012* | **Modified provisions related to blacklisting and disconnection of telecom resources:** in 18(5) for disconnecting telecom resources provided to RTM for sending promotional messages only in case the RTM blacklisted for sending promotional messages but in case of transactional messages, both the telecom resources for transactional messages as well as promotional messages to be disconnected Blacklisted Telemarketer will not get any telecom resources during the period of blacklisting. |
| 10 | *10th Amendment*<br><br>*Dated 5th November 2012* | **Introduced signature solution to detect UTM**: It was observed that UTM generally send bulk promotional SMS as SMS blast using special equipment and software applications. To identify bulk promotional SMS, in Regulation 2, the definition of **signature** was added as contents of commercial communications having **same or similar characters or strings or variants** thereof but does not include subscriber related information.<br><br>**Modified format of registering a complaint:** In 19(4) dropped the requirement of mentioning the particulars of time of receiving UCC while registering a complaint.<br><br>**Introduced higher tariffs for SMS in bulk:** In 20(2), To make it economically unviable to UTMs for sending commercial communication rate not lower than the rate specified in Schedule XIII of Telecommunication Tariff Order (TTO) 1999.<br><br>**Introduced restrictions on SMS/hour**: restricting that no SMS having similar signature and more than 200 SMS/ hour delivered through its network except for RTM or TMSE; |

IndiaCode

| | | |
|---|---|---|
| | | **Introduced 'Web-based UCC Complaint lodging system'** and dedicated email address to lodge UCC related complaints.<br><br>**Added process to intimate for disconnecting resources:** in Schedule-V (13), in addition to NTR for disconnecting resources, instructions received from NTR/ TRAI.<br><br>**Modified format for registering a complaint:** Schedule VI (4): Appending telephone number or header to SMS with or without space after a comma |
| 11 | *11th Amendment*<br><br>*Dated 23rd May 2013* | **Modified definition of signature:** changed to 'Characters or strings, or variants thereof, of a commercial communication and does not include subscriber related information'<br><br>**Introduced Transactional SMS charge**: charges payable by an OAP to the TAP for each transactional SMS sent by an RTM or TMSE.<br><br>**Introduced cases for the exemption** for "Transactional SMS charge" |
| 12 | *12th Amendment*<br><br>*Dated 24th May 2013* | **Introduced provisions for blacklisting:**<br><br>Modified Regulation 13(2), 18(3) for blacklisting customers and RTMs and communicating to all access providers to disconnect telecom resources.<br><br>**Introduced power of the Authority to restore resources:** Regulation 19A introduced that the Authority may direct the Access Provider to restore all the telecom resources of a subscriber and delete the entry in the blacklist. |
| 13 | *13th Amendment*<br><br>*Dated 22nd August 2013* | **Introduced process to complain on behalf of others:** Regulation 19(4), enabled to complain on behalf of others by adding details of the person on whose behalf complaint is being made to the brief description of such UCC.<br><br>**Included to issue notice to person causing to send UCC and provision for disconnection of his telecom resources:** Regulation 19(11) added that if UCC has solicited commercial transaction on behalf of a person on the same mobile number or different telephone number then issue notice separately to such subscriber or person other than the subscriber making UCC. After 2nd notice, disconnect all telecom resources of that subscriber.<br><br>**Introduced to submit details of all bulk connections:** Regulation 20(2)(p) introduced to submit details of all bulk connections provided during the previous calendar month.<br><br>**Introduced financial disincentives to access providers on account of UTM activities:** Regulation 22(1A) introduced that for UCC from UTM, OAP liable to pay an amount, by way of financial disincentive, not exceeding Rs.5000 for every such complaint. |

IndiaCode

| | | |
|---|---|---|
| 14 | *14th Amendment*<br><br>*Dated 3rd December 2013* | **Introduced procedure for renewal of registration of telemarketers and requirements of security deposits** Regulation 14(3) changed registration period from three years to five years<br><br>Regulation 14(4) added: registered telemarketer may apply for renewal on the same terms and conditions, sixty days before to the expiry of its registration and paying specified fee.<br><br>**Introduced power to amend schedules specified in Schedules and make it effective within time limits** Regulations 20(2)(a) and (b) proviso added regarding amending Schedule-V and accordingly modifying agreement(s) between AP(s)and RTM(s) within the specified time. In Schedule-III modified regarding fee(s) and security deposit requirements. |
| 15 | *15th Amendment*<br><br>*Dated 7th April 2014* | **Introduced power of the Authority to restore telecom resources** Regulation 19B: Restoration of disconnected telecom resources- on a request made to the Authority and satisfying the Authority about reasonable steps taken to prevent recurrence of the contravention, the Authority may order restoration on payment of Rs. 500 for restoration of each telecom resource. |
| 16 | *16th Amendment*<br><br>*Dated 10th December 2014* | **Modified definition of header**<br><br>Regulation 2(m) modified to include alphanumeric or numeric identifier<br><br>**Modifed definition of transactional messages, defined sending entities, conditions for sending and recipients for such messages**<br><br>Regulation 2(ab) (iiiA), (iiiB), (iiiC), (iiiD) added to define transactional messages, sending entities and recipients for such messages as information sent by:<br><br>- e-commerce agencies in response to e-commerce transactions made by their customers;<br><br>- a company or a firm or depository participant, registered with SEBI or IRDA or AMFI or NCDE to its clients pertaining to the account of the client;<br><br>- a registered company to its employees or agents or customers pertaining to goods or services provided by it.<br><br>- a registered company or charitable trust or society or TSP, pertaining to its services or activities to the telecom subscriber in response to a verifiable request of such subscriber.<br><br>**Introduced provisions for the option to reply messages**<br><br>Regulation 17(4) proviso added: telemarketer for receiving a reply in response to the transactional message, to enter into an agreement with the Access Provider under Schedule-VII and Regulation 17(10) proviso added for such telemarketer to have the facility of receiving incoming SMS. |

indiacode

| | |
|---|---|
| | Regulation 19(8)(a) & in Regulation 20(2)(b): Schedule-VII added for Agreement between Access Provider and Transactional Message Sending Entity (TMSE) to have a facility for the reply message, when such Transactional message do not fall within the definition of promotional message.<br>**Introduced provisions for taking request from the customer for sending transactional messages**<br>TMSE shall<br>(a) send information only after receipt of a verifiable request<br>(b) information will be provided for a maximum period of six months unless renewed and also process to opt out from receiving such information;<br>(c) obtain afresh request every six months for continuing<br>(d) intimate procedure to opt out from receiving such information and in every advertisement wherein the details of its services and activities are published<br>(f) maintain a record of the request<br>(g) not send any objectionable, obscene, unauthorized content, message or communication |

1.4.2 Key points of UCC Directions issued by TRAI are as below:

| S.N. | Direction related TCCCPR 2010 | Key points |
|---|---|---|
| 1 | *Direction dated 27th September 2011;*<br>*Direction dated 23rd December 2011;*<br>*Direction dated 25th January 2012;*<br>*Direction dated 26th June 2012;* | **Exemption from the limit of one hundred SMS per SIM per day for non-commercial communications categories.**<br>• excluded following:<br>(i) Dealers of the TSPs and DTH Operators for sending a request for an electronic recharge on mobile numbers;<br>(ii) e-ticketing agencies for responding to e-ticketing request<br>(iii) The social networking sites for sending SMS to its members pertaining to activities relating to their accounts<br>(iv) Agencies providing directory services<br>• exclude all machine to machine and person to machine messages, where the machine is not a mobile handset and no manual intervention is required at the receiving end. |
| 2 | *Direction dated 25th October 2011;*<br>*Direction dated 23rd December 2011;* | **Introduced Categories of SMS as a Transactional message:**<br>Information sent by<br>(i) e-commerce agencies in response to transactions<br>(ii) a company or a firm or depository participant, registered with SEBI or IRDA or AMFI or NCDEX or MCX to its clients |

IndiaCode

| | | |
|---|---|---|
| | | (iii) a registered company to its employees or agents or to its customers pertaining to services or goods to be delivered<br><br>(iv) a registered company or charitable trust or society or TSP in response to a verifiable request of such subscriber;<br><br>Sends information only<br><br>(a) after a verifiable request and maintain a record for 3 months<br><br>(b) for a maximum six months, unless renewed<br><br>-intimate the procedure to opt out in every advertisement wherein regarding the facility is published by it in any media;<br><br>-no objectionable, unauthorized content and no mixing of UCC or promotional message with the information |
| 3 | *Direction dated 20th January 2010* | **Introduced Blocking of bulk international message.**<br><br>(i) no incoming international SMS containing alphabet or alphanumeric header as a CLI is delivered through its network;<br><br>(ii) no incoming international SMS containing the originating country code +91 is delivered through its network;<br><br>(iii) except on 'blackout days' no incoming international SMS with more than 200 SMS/hour, having similar 'signature' is delivered<br><br>(iv) global titles of only the network of those entities with whom the Access Providers have entered into agreement are allowed. |
| 4 | *Direction dated 10th August 2017* | **Sub: Unsolicited bulk SMSs relating to investment in securities market.**<br><br>Access Providers to<br><br>• make necessary arrangements to filter and block particular type of SMSs using Signature solution<br>• ensure before sending any SMS relating to investment advice or tip verify that the message is sent in accordance to the SEBI's requirements |

## 2 Key issues and concerns raised for seeking inputs

### 2.1 Issues and Concerns with the current regulatory framework

2.1.1 Despite taking various measures, UCC related complaints are on the rise and the problem is not fully under control. Provisions of blacklisting and introducing signature solutions in the network helped initially. Introduction of DND Mobile App by TRAI is a very convenient way for the customers to report about UCC complaints. More than 2 million complaints have been received so far and recent average of complaints is approximately 40 thousands per month. Since introduction of provisions for disconnecting telecom resources, approximately 1.4 million numbers have been disconnected while during February 2018, about 14 thousand numbers were disconnected. About 460 thousand numbers have been blacklisted so far. Despite disconnecting more than a million telephone numbers, UCC is not fully under control.

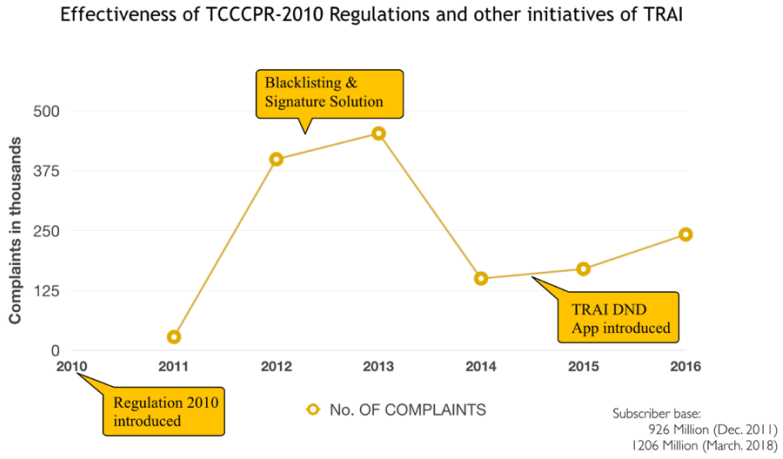



*Figure 1: UCC Complaints over last few years*

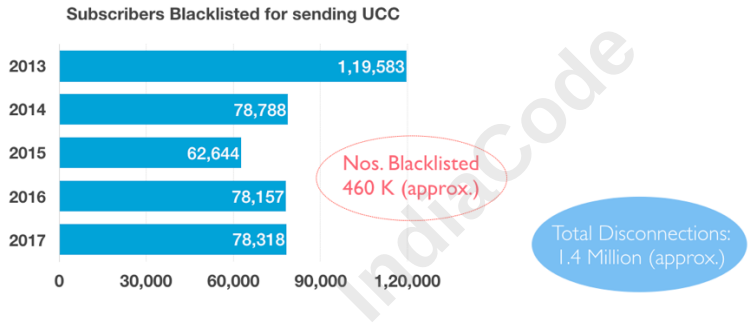



*Figure 2: Disconnection of Telecom resources for sending UCC*

2.1.2 Various problem areas which are related to effectiveness and efficiency of the current regulatory framework have either been observed or came into notice are:

i. *The existing system takes about 24 hours to register preferences and requires up to seven days to enforce the revised preferences,*

ii. *Usually time required to resolve UCC complaints and take action against defaulter is more than seven days. This long-time window is exploited by the unregistered telemarketers to send UCC,*

iii. *Despite measures taken by the TSPs to control UCC from Unregistered Telemarketers (UTMs) and provisions in the regulations for the disconnection of telecom resources, UCC from Unregistered Telemarketers is still continuing,*

iv. *Due to false complaints or fake identities against which connections are taken, the telecom resources of person who might not have indulged in sending UCC are sometimes disconnected.*

v. *Intuitive and Intelligent Mobile App for registering preferences and making complaints is required for most Operating Systems and Platforms in the mobile device market, which would enable device users to make complaints against the sender of UCC in a convenient and user friendly manner,*

vi. *The existing system takes a long time to make preferences made by the customer effective,*

vii. *Cases where the request (consent) is taken by organizations or individuals to send transactional messages are unverifiable and accessible, as well as, customers don't have the choice to revoke such consent,*

viii. *Transactional Message headers are abused to send promotional messages,*

ix. *Cases of non-traceability of Senders of UCC, and intermediaries,*

x. *Cases brought to notice by SEBI and RBI about UCC messages related to financial, trade and security market (by unauthorized entities)*

xi. *New ways used by telemarketers to make UCC, such as robocalls and silent calls which may be of concern to the customer.*

2.1.3 To address various issues and concerns, some of them highlighted above, Consultation Paper on Unsolicited Commercial Communications (UCC) was issued on the 14th of September 2017. In response to this consultation paper, comments from 29 stakeholders and counter comments from 2 stakeholders, including Access Providers, Associations, Telemarketers, Solution Providers and consumer organizations were received. Subsequently, Open House Discussion (OHD) was held on 15th December 2017 at Delhi.

**2.2** Key issues deliberated in the consultation paper: **Consultation paper mainly focused on bringing efficiency and effectiveness in System for Customer Preference Registration, System for Registration of Related Entities (including Consents given by the customer to senders) and System for Complaint Handling. Summary of key issues for consultation is given below:**

2.2.1 29 questions were raised in the paper for consultation. Out of 29 questions, 7 were mainly related to Customer Preference Registration System; 9 were related to the registration system for related entities, while rest 13 were related to Complaint Handling System.

2.2.2 There are a few issues which may be interrelated with multiple aspects e.g. Scrubbing as a Service may be useful to improve gap between time when preference was opted by customer and time it came into force, and it may also be helpful to improve gap between time when UCC complaint was made and its resolution.

## 3 Inputs, analysis and conclusions on issues related to Registration System for related entities

### 3.1 Issues related to Registration System for related entities

3.1.1 **Robust verification and authentication of telemarketers**: It is noticed that in case of unauthorized activities or violations of the regulations, it is often difficult to trace defaulting telemarketers and sender (i.e. content provider). This points to the need for clearly demarcating roles and responsibilities of various stakeholders in the value chain and for formulating mechanisms to make them traceable. This will require changes in the process of registration of RTMs and a process for robust verification and authentication.

3.1.2 **Registration of Intermediaries, Principal Entities and their agreements**: In addition to telemarketers, several other entities are involved in the origination, transmission, processing and delivery of commercial communications, which can make it difficult to establish responsibility in case of violations of UCC regulations. Therefore, it might be necessary to register all such entities and intermediaries, such as Senders or content providers, TMSEs, Principal Entities, aggregators and others. It might also be necessary to specify Standard agreements between entities in the chain.

3.1.3 **Registers and Registrars for different purposes, e.g. assigning headers, recording consents, registering consent/ content templates and execution of agreements**: RTMs often communicate with those who have opted out of commercial communications on the ground that the consent of the recipient has been obtained for such communication. However, records of such consent are not available in a digital form. Further, this consent information is not considered during scrubbing. Instances of mixing of transactional messages with the promotional messages have also been observed. In such cases,

telemarketers express their inability to inspect every message passing given their very high volume. One approach to tackle both these issues would be to mandate pre-registered content templates and consent templates. Then technological solutions can be deployed to ensure that the consent obtained, or the contents of a transactional message are in line with regulations. Headers may also be registered, and suitable rules developed for assigning the headers. To manage all these functionalities, it will be necessary to establish dedicated, trusted entities (registrars), who can operate a network for sharing, managing and storing information in a secure manner. The registrars and the network need to be able to handle header registration, execution & management of contract agreements among entities, managing and recording consent taken by TMSEs, recording content templates and verifying the content of transactional messages. The networks and functions can be operated and managed either by an independent agency or by TRAI. In case of agencies other than TRAI, these functionalities may be operated on an exclusive basis or based up on specific functions to be performed. Each of the functions could be provided by service providers who may charge them. TMSEs would expect these functional entities to protect their client database. Further, it is necessary that consent given by customers be recorded in an immutable and non-repudiable manner.

3.1.4 **Implementation phases of new system**: Implementation of new systems may either be full-fledged or in a phased manner. Constitutional bodies, government organizations or other entities may also participate in the system based on their need and option.

3.1.5 **Securing Preference Data**: Unscrupulous telemarketers and other intermediaries may deliberately leak preference data to unregistered telemarketers or data may also leak out because of inadequate measures taken by RTMs or intermediaries to protect or secure data. Therefore, it is necessary to devise a mechanism to ensure that preference data or consent data used to scrub is protected. Scrubbing as a service model could be useful for doing so. OTP based authentication for queries made by individuals may be introduced for protecting preference or consent data. Other mechanisms may also be adopted to protect the data.

3.1.6 **Changes in the Header Format and Structure**: Headers are useful for the recipient of the commercial communication to identify sender, and for presentation of the content as a thread or at a single place, making it convenient for the customer to manage the content on his or her device. Headers may also require change in its format and structure to deal with new requirements of preferences, entities, or purpose. Headers may also be assigned in blocks to principal entities and different charges may be levied for a block of headers. Guidelines and mechanism shall be required for avoiding proximity match of headers with well-known entities while assigning the headers.

3.1.7 **Managing Header Assignments by Principal Entities for their DSAs**: Presently Direct Sales Agents (DSAs) or agents authorized by principal entities register themselves as telemarketers. DSAs or such agents independently acquire headers for carrying out commercial communication activities. Although they work on behalf of the same principal entity, action only lies against the individual header assigned to a DSA or an agent. Principal entities may be required to take control of commercial communication activity being done on its behalf. Telemarketer registration system and header assignment process would thus require enhancements to provide more flexibility and better control to principal entities over their Direct Sales Agents (DSAs) or authorized agents to whom they have delegated commercial communication related functions. New system may provide capabilities to Principal entities to manage header assignments to their DSAs and authorized agents. It may also provide better control and management of header life cycles assigned to DSAs and authorized entities.

3.1.8 **Transactional Voice Calls for Senders and technology solutions to display identity to the recipients**: There are instances where RTMs or TMSEs have reasons to contact customers (who have opted out of commercial communications) via voice calls for justifiable and legitimate purposes. In such cases, it is

IndiaCode

necessary for customers to know who is calling, even when the name of the calling party is not in the address book of the recipient. Display of calling line identity in a way which is easily recognizable and displayed after authentication may be useful. It is also desirable for organizations, government agencies and companies to forward their identity to a call recipient together with the call. This may require a robust mechanism to identify voice calls from particular organizations, e.g. by allocating dedicated numbering series to these entities or by using Intelligent network-based solutions or using capabilities of IP Multi-Media Subsystems. Solutions may also be required for providing flexibility to TMSEs to operate it and control its authorized entities.

3.1.9 **Restoring sanctity of the Transactional Messages**: It is observed that transactional messages and promotional messages are sometimes being mixed. It is necessary that before sending commercial communications, clear distinction is made about its category and the purpose for which it is sent. A better method for labelling it with the associated category and purpose is required. Sanctity of transactional SMS needs to be restored as they may only be such messages as are time critical and not promotional in nature.

### 3.2 Comments of Stakeholders

3.2.1 **Robust verification and authentication of telemarketers:**

i. *Almost all stakeholders supported the idea of change in the registration process in order to create a robust mechanism. Two of them opined that the email and phone numbers of telemarketers should be authenticated through one-time password **(OTP)**.*

ii. *Some stakeholders suggested that that telemarketer should declare the origination of calls/SMS by sharing latitude-longitude context **Geo-tagging**. One of them added that specific **app like "authenticator"** from Hotmail / google can be used. During OHD, one of the solution providers suggested that **Block chain technology** can be used to make the entities traceable.*

3.2.2 **Registration of Intermediaries, Principal Entities and their agreements**:

i. *Almost all stakeholders supported the idea of **registration of principal entities and TMSEs.** Some supported that **registration of aggregators** should also be done.*

ii. *A few stakeholders were of the view that registering new entities will not bring in additional effectiveness. They were of the view that it could in fact **be counterproductive, since having** too many registered entities in the chain will lead to as many **disputes. They were also of the opinion that this would make it more difficult, rather than less, to establish accountability**. However, stakeholders were divided on this issue and some were in favour of registration of content providers and other entities while others were opposed to it. Stakeholders in favour of registration argued that doing so will improve traceability and accountability.*

iii. *Majority of stakeholders supported having standard agreements for principal entities, intermediaries and content providers or senders. One stakeholder mentioned that while Telemarketers are responsible for all the telemarketing activities initiated by them, they should ensure that other entities with whom they are in a business relationship **enter into standardized agreements** and they should also be responsible for the consequences of non- compliance and standardized agreements will enable it. **Few rejected registrations and standard agreements for currently unregistered players on the grounds that performances would be impractical**.*

iv. *Stakeholders also recommended incorporating the **RTM's license number in an encoded form, at every step of the process**.*

3.2.3 **Registers and Registrars for different purposes e.g. assigning headers, recording consents, registering**

**consent/ content templates and execution of agreements**:

i. *Responses from stakeholders on the issue of header registration were mixed. Some stakeholders supported the idea of header registration with a central registry whereas some opposed it in favour of the current process of TSPs assigning header to the RTMs and TMSEs. In the current process, the RTMs and TMSEs are required to maintain the records related to header assignment.*

ii. *One stakeholder added that a number of commercial communication messages are being observed to have promotional content under transactional headers. This can be curtailed by mandating the TMSEs to* ***deploy anti-spam systems*** *in their platform to identify and block messages basis keyword/ phrases etc.*

iii. *Regarding the establishment of Consent Registrar and recording consent in a verifiable, immutable and non-repudiable manner, many stakeholders supported the idea of creating newer and* ***smarter systems for handling and managing consent****. Stakeholders supported the idea of having a* ***centralized system*** *for carrying out the proposed functions. One of the TSPs also supported the idea of creating* ***universal portal*** *where every RTM, aggregator, or entity who takes consent from a customer (either through physical form, website, application or email) may* ***upload a request.*** *This system in turn should trigger real-time notification to the customer through SMS. Another TSP proposed that the Authority* ***suggest a reference template for recording the explicit consent*** *of the customer, they further suggested, that TMSE should share the template and* ***TRAI*** *or* ***any agency appointed by it should audit the template*** *on a regular basis.* ***Another view*** *was that consent taken by customers can be maintained at an outsourced vendor's end on a cloud platform/server & checks/****verifications can be on a case to case basis*** *– The cost of maintaining the consent and its ready retrieval can be* ***covered by the content providers/business entities.***

iv. *Some other stakeholders from the telecom industry, however, indicated that the* ***present systems were working adequately****. One of the stakeholders was of the view that requiring consent forms to be uploaded on a central repository may not be feasible. They argued that* ***consent*** *is usually taken as* ***part of a larger service contract*** *as individual contracts* ***cannot be signed for every term/condition****. Such contracts may, therefore, contain* ***commercial secrets and personally identifiable information****, which are not relevant to this purpose. Further, such consent is often taken in the form of an* ***electronic click-wrap agreement****. Uploading of such electronic templates will* ***not serve any purpose*** *and will* ***merely increase the workload and costs for delivery of services****. They were of the view that consent forms should be* ***demanded ex-post during an investigation*** *of a complaint and a case-by-case review of this nature* ***would be more efficient and cost-effective****. Another industry stakeholder suggested that uploading of consent taken by TMSEs carries the risk of* ***compromising customers' privacy or the business entity's commercial secrets.***

v. *One of the stakeholders informed that it uses telecom services for the purpose of Membership with its political party and they had launched a nationwide* ***'missed call' campaign to enroll new members****. They use a toll-free number for the membership drive. Here, the* ***missed calls are considered as consent for opt-in*** *given by any person (subscriber of that mobile number) for membership and for receiving political campaign and information dissemination from the party to its members.*

vi. *Three stakeholders responded to this question on content templates and all three* ***supported the idea****. Majority of the stakeholders supported the idea of* ***TRAI creating and operating the system****. The need for centralization for administering such a complex system was quoted as the reason for supporting this stance. Stakeholders also commented that* ***Content approval may cause significant delay and disruption*** *as companies often make* ***minor tweaks in templates*** *to make*

Indiacode

*improvements.*

3.2.4 **Implementation phases of new system:** Most of the stakeholders have supported implementation in a phased manner. Few stakeholders are of the view that there should be a trial period, during which participation must be **voluntary for entities other than TSPs**. One of the telemarketers has suggested that a time frame of **3-6 months** be given to all entities to comply. Till then, the business must be allowed to run **in parallel with the old system**.

3.2.5 **Securing Preference Data**:

i. *Several of the stakeholders also agreed with employing scrubbing as a service model to protect customer data. Out of these, some stakeholders fully agreed with OTP based authentication for granting access to NCPR data while one solution provider opined that OTP based authentication cannot adequately address data protection concerns. Few stakeholders recommended authentication based on cryptographic keys. One of stakeholders* ***recommended application environment isolation through secure service containers to protect customer data*** *(even from system administrators). One of the stakeholder recommended* ***storing data in encrypted form with a one-time mapping of real phone numbers to proxy numbers****, which can only be used once. This can be part of scrubbing services. Some recommended inserting data protection and confidentiality obligations in the standard agreements between access providers and RTMs. Further, some stakeholders opined that there is no need for a separate data protection regulation at all.*

ii. *Most of the TSPs have supported the Scrubbing as a Service model. One TSP was of view that it might increase the cost of scrubbing. Solution providers have commented that scrubbing as a service on a dynamically updated database may* ***reduce any disputes*** *that may result in time lags and provide* ***clear audit logs****. A few stakeholders have commented that it may* ***introduce delay****.*

iii. *Several TSPs agreed with the idea of having authentication through OTP for scrubbing, to make NCPR (National customer preference register) data more secure. Few stakeholders also suggested that* ***OTP based authentications*** *should be mapped with date and time as primary key which should be* ***valid for a particular period****, not exceeding 24 hours. Few stakeholders recommended authentication based on cryptographic keys. One of stakeholders recommended application environment isolation through secure service containers to protect customer data (even from system administrators). One of the stakeholders also recommended to store data in encrypted form with a one-time mapping of real phone numbers to proxy numbers, which can only be used once. This can be part of scrubbing services. Some recommended inserting data protection and confidentiality obligations in the standard agreements between access providers and RTMs. Further, opinion received that there is no need for a separate data protection regulation at all.*

iv. *One Stakeholders* ***disagreed with the scrubbing as a service model****. It noted that all the TSPs and telemarketers should be connected with a* ***central registry using an API*** *so that any registration, change or deregistration of subscriber preferences can take place on a real-time basis and be noted by the Authority, obviating the need for scrubbing as a service.*

v. *Among other stakeholders, some recommended having a* ***common access system*** *for all TMSEs, with authentication systems for TMSE. Others recommended authentication based on* ***cryptographic keys****. Both also recommended* ***selective access to TMSE client databases****, based on the identity of the agency trying to get access, and registered preferences of customers. Few recommended* ***storing encrypted logs of TMSE transactions*** *in order to enable regular audits.*

3.2.6 **Managing Header Assignments by Principal Entities for their DSAs:** Most of the banks and other stakeholders **supported** this. They expressed that extending capability to manage header assignments

Indiacode

to them will help them to better control and manage headers assigned to their DSAs or any entity authorized by them to perform commercial communication functions on their behalf.

3.2.7 **Changes in the Header Format and Structure**:

i. *Most of the stakeholder have commented that headers assigned by RTMs / TMSEs to Principal Entities should be unique. One of the entity has suggested Header format as* ***<Name of entity> - <operator><operator code><unique 3-digit TM code given>****.*

ii. *Few other service providers have commented that* ***first two digits*** *of the header should clearly convey the* ***nature of communication like 'PR'*** *for promotional communication and 'TR' for transactional communication followed by organization's header. They suggested an increase in the length of header up to 11 digits for covering maximum entities with unique headers. It should be the web-based interface* ***like domain name registration for the header assignment****. They also recommended automatically revoking the authorization for headers which remain unused for a period of 6 months or more. Additional characters should be allowed to be incorporated in the headers to* ***avoid proximity match of headers with well-known entities****.*

iii. *One service provider has suggested having 11 characters headers of the form* ***XX-AAAAAABBB where***

- The first two characters 'XX' may denote **TSP and Circle** from where the message is being sent
- Character '–' may act as a **separator** between the TSP and Content Provider
- 'AAAAAA' may be the identity of the Content Provider, 'BBB' may denote the **aggregator/end user** on whose behalf RTM/TMSE has sent a message

iv. *Stakeholders suggested that* ***shorter length of header allotment to PEs*** *and the responsibility of* ***checking the proximity issue*** *should be* ***with PEs****. Well-known entities like banks and financial institutions should* ***declare all headers used by them*** *and also provide the* ***possible misleading headers*** *with proximity to such headers to NCPR portal through their service providers. The portal can disallow allocation of proximity headers basis the merits of the case. Some stakeholder suggested that* ***Additional characters*** *should be allowed to be incorporated in the headers* ***to avoid proximity match*** *of headers with well-known entities.*

v. *Further suggestion received was that the proximity match could be resolved on the* ***same principle as*** *wherein* ***first preference*** *should be given to party having* ***registered trademark for a particular brand name*** *and in case* ***neither party*** *has a registered trademark then the party who has* ***first put to use*** *the said brand name would be given preference over the other party(ies).*

3.2.8 **Transactional Voice Calls for Senders and technology solutions to display identity to the recipients**:

i. *Most of the service providers,* ***except few****, have* ***supported*** *the idea of permitting TMSEs to make voice calls. They also supported the allocation of* ***separate number series for TMSEs****. One service provider has commented that segregation already exists for promotional calls.*

ii. *Few stakeholders have commented that it may provide ways to customers to identify calling TMSE. It may provide flexibility to TMSEs in operating it and give them better control on their authorized entities.*

iii. *Some stakeholders had the opinion that in case of permitting transactional voice calls:*

- It should be allowed only for pure transactional purposes
- Customers may be provided with an option to opt-out of such voice call
- Measures may be required to be taken to ensure that there is no scope for misuse
- It may lead to complaints regarding usage of transaction pipe for promotions

IndiaCode

iv. *One of the stakeholders suggested solutions to identify calling TMSE using Intelligent network (IN) or IP Multi-media subsystem (IMS) based solutions.*

v. *Another stakeholder suggested that the regulation should mandate the registration of intermediate DSAs and authorized agents by the Principal Entities. For any non- compliance by DSA's, PE will be held responsible. All the stakeholders supported the view that there must be a provision of content template via which misuse of transactional pipe can be controlled.*

3.2.9 **Restoring sanctity of the Transactional Messages**:

i. *Few stakeholders requested that the **definition of transactional messages be relaxed**, and that it should include communications and offers from opted-in entities as regards their products and offers. Such a move will allow customers to benefit by getting alerts and updates on offers from the Brands they regularly transact with and with whom they have already registered to receive periodic alerts and updates.*

ii. *All TSPs side stated that TRAI has mandated them to provide information to the customer in addition to their monthly bills, such as details of nodal officer, toll-free complaint number etc. Further, if messages regarding balance deduction from bank contain information about related product such as a loan, may not be an inconvenience to the customer. Therefore, they recommend that such additional information related to product or service in authorized transaction communication should not be treated as UCC.*

iii. *Regarding how to segregate the transactional message of critical nature with others, Stakeholders suggested that **Header categories as CRITICAL** or OTHERs should be defined. No mixing of transactional and promotional should be allowed. Govt. and semi-Govt. entities, which will send messages in future, must be listed out.*

Uncode

### 3.3 Analysis of inputs and conclusions

Following paras deliberates on the issues which are related to Registration of related entities in reference to UCC eco system. Issues and responses to the questions raised in the consultation paper are also summarized. Key points from the current regulatory approach and approaches taken in other jurisdictions to deal with the issues were also considered while analyzing inputs and concluding the issues. Analysis of inputs and conclusions of the Authority are as follows:

3.3.1 **Prescriptions that are too prescriptive lead to frequent amendments and yet slow response:** Before delving into specific issues related to the registration of entities, it is necessary to understand the previous regulatory approach to deal with the UCC issues. Table mentioned in Para 1.4 of this explanatory memorandum provides summary of key changes made in the regulations since year 2010 when current main regulations came into force. It would be observed that changes made in the regulations were to respond to the changing characteristics of senders of UCC. Despite a large number changes, their nature, and the frequency with which such changes were made, the problem of UCC persists. It indicates the need for a flexible and adaptive approach, where the framework evolves in responses to new challenges.

3.3.2 **Co-regulation approach may be more effective in case of UCC:** Dealing with UCC, however, does require detailed procedures, the setting out of clear roles and responsibilities and prescriptions for holding defaulting entity to account. Though, prescribing such details in the regulations has led to problems indicated above. These conflicting requirements can, perhaps, be met by a co-regulatory approach where the access provider develops and administers arrangement of involved entities through codes of practice, while regulations lay down the principles and the desired outcomes rather than avoidable details. In addition to this, the regulations would circumscribe and enable the access providers

to enforce appropriate arrangements.

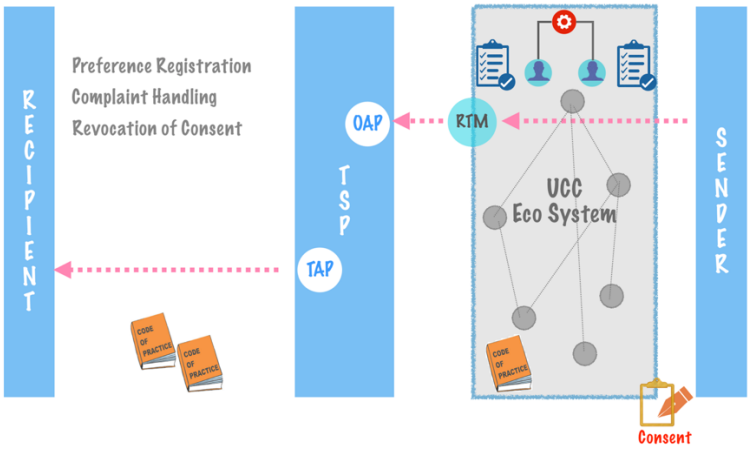



*Figure 3: Eco System for Commercial Communications*

3.3.3 **Code(s) of Practice (CoPs) provide evolving and adaptive framework**: It is proposed that CoPs be formulated and operated by the access providers as per their requirements, who may specify terms and conditions for agreements with entities and action to be taken when an entity fails to perform the desired role or carry out its responsibilities. With a co-regulatory approach and codes(s) of practice by the access providers the governance framework can evolve over time, as needed. This would provide the access providers flexibility in developing the system to attain regulatory objectives. The issues listed below are to be dealt with in a Code Practice (to be called the Code of Practice for Entities or CoP-Entities) to achieve regulatory objectives in conformance with the regulations:

i. *details of the requirements for robust verifications and authentication mechanism of telemarketers,*

ii. *registration of entities,*

iii. *establishing system in this regard,*

iv. *securing the data,*

v. *offering services to the senders of commercial communications,*

vi. *flexibility to principal entities to manage headers,*

vii. *assigning headers,*

viii. *header format and structure,*

ix. *identity display to the recipients,*

x. *Categorization of content types etc.,*

xi. *role and responsibilities of participants,*

xii. *processes for safe and secure handling of data,*

Access provider should enforce provisions in the CoP-Entities by entering into agreements with the participating entities and ensure compliance using technology driven solutions.

While finalizing header format and structure of header, it may be ensured that numbering series is in accordance to the as per National Numbering Plan of DoT or any directions or guidelines issued in this

Draft Code

regard. Currently 140 series is assigned for telemarketing promotional calls and level "5" is allocated to access providers to assign short codes. Level "1" short codes for messages are being assigned by DoT which are accessible across access providers. Under current regulations, level "5" is also used to provide reply path to the customer to respond against received commercial communication, same may be considered while formulating codes of practice. To ensure that senders obey the regulations and in case of default, actions may be taken against them and licensing requirements for International Long Distance traffic, senders originating commercial communications outside from the country would route traffic via International Long-Distance Operators (ILDOs) as being done at present. **In view of this, the Authority decided to specify similar provisions in the regulations for ILDOs to block traffic related to bulk messages.**

3.3.4 **Unbundling and delegation of functions**: Registered Telemarketers (RTMs) at present carry out multiple functions, such as scrubbing against record of preferences, checking against records of consents provided by principal entities, delivering messages or voice calls, etc. Under the revised regulations more functions are required, such as consent acquisition, entity registration, etc. Unbundling of composite functions as independent functions and introducing new functions, which can also be independently performed, provide opportunities to new players to participate in the UCC eco system and offer existing players to shed any role they do not wish to perform.

3.3.5 Access Provider may be required to define functions referred to in the above paras in more detail. Interactions among these functions and information exchange processes are also to be prescribed in CoP-Entities, some of the key functions which will have to be defined and performed are:

i. Header Registration Function (HRF)

ii. Consent Registration Function (CRF)

iii. Content Template Registration Function (CTRF)

iv. Scrubbing function (SF)

v. Content Verification Function (CVF)

vi. Delivery Function for Messages with Telecom Resource Connectivity to Access Provider (DF)

vii. Aggregation Function for Message to other Telemarketer for delivery function (AF)

viii. Voice Calling Function with Telecom Resource Connectivity (VCF)

Each function has to generate activity logs for the actions performed with such functionality irrespective of the other functions performed by the same or different physical entity. Users taking services of such functions may be provided options to carry out individual functions from same or different physical entities. Further specific details about the roles to be played under these functional entities may be included in codes of practice which are to be formulated by access providers.

3.3.6 **Flexibility to customize the agreements and requirements**: UCC eco system would be multi layered and participating entities may play single or multiple roles. Scope of such entities may be quite different from each other, and to more effectively or efficiently perform a function, an entity might take additional specific measures over and above those specified in the regulations or codes of practice. In such scenarios, it would not be practically possible to define procedures, fees and actions to be taken against participating entities in a prescriptive manner. Granting flexibility would help make the system more agile and adaptive in response. Codes of Practice are to be formulated and submitted by access providers in a manner that fulfils the purpose of the regulations. In case of deficiencies, Authority may instruct access provider(s) to make changes in the formulated codes of practice. Any attempt to misuse vested power by any of the participating entities would be dealt with by market forces, as participants

IndiaCode

would have the option to take connectivity from any access providers. In time, there may develop customized legal agreements that serve the needs of all parties in a specific instance.

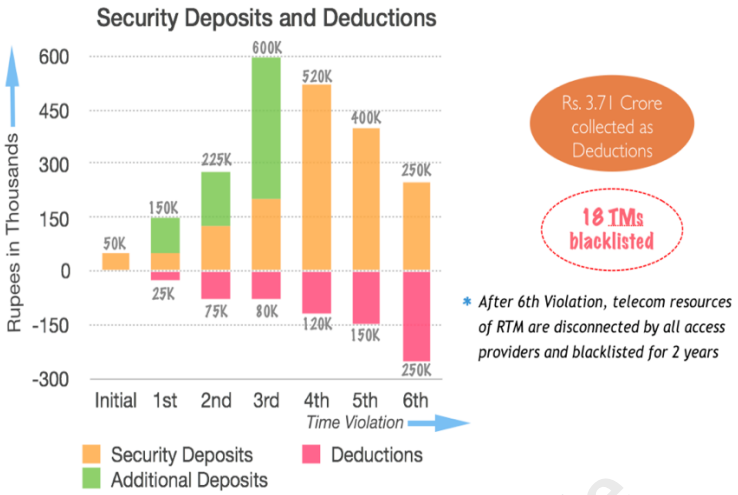



*Figure 4: Provisions in existing regulations for deposits and deductions in cases of non compliances by tele-marketers*

3.3.7 **Code of Practice for Preferences (CoP-Preferences) similar to CoP-Entities**: Like Code of Practice for entities (CoP-entities), access provider(s) would formulate Code of Practice for Preferences (CoP-Preferences) to deal with the details of categories and to enable setting up of preferences. Over time they may evolve to include more categories or sub-categories, bands of time, types of day, modes of communications, etc. However, expansion of categories or sub-categories would need to be in a manner that customers who have previously exercised their choice do not have to unnecessarily exercise that choice again. Expansion of set of choices for content types would require more refined categorization of the communication at the time of scrubbing, delivery, etc. The requirement of expanded choices would also require corresponding evolution of CPRF, DL-Preferences, scrubbing process, complaint handling, etc. As discussed in case of CoP-entities, the main regulations only contain regulatory objectives and enable the choices to evolve, while details of the choices and their enforcement remain part of code of practice.

3.3.8 **CoP-Preferences to also include requirements of Consent and Revocation of consent:** Just as for preference, the scope of consent would also evolve. Consent may require registration of templates that define the consent and customers may revoke their consent, if it doesn't serve their purpose. Consent is currently taken in various forms, e.g. punching telephone number in the computerized form at the time of making payment or while taking feedback about the goods or services. There is no robust mechanism to verify the ownership of number provided by the client at the time of giving consent. Verification of consent at a later stage poses two challenges: first to retrieve the information from TMSE database, and second, to verify the authenticity of the recorded consent. Robust mechanism for recording the consent is required to be developed and deployed in which the consent is explicit and recorded in a verifiable and robust manner. It may reasonably be inferred as consent when the transmitted information is related to a transaction, including a specific inquiry about the product or service. In such cases, it is not practically possible to take prior consent and it is not in the interest of the customer to block such communications.

3.3.9 **Consent Acquisition and Consent Registrar**: Consent acquisition requires authentication of the target recipient and may be implemented by using OTP. Further it must be recorded in an immutable and non

TRAI Code

repudiable manner. In case of explicit consent, recorded consent must be available as a part of consent register. To facilitate this, a Customer Consent Recording System needs to be established where a consent register is maintaintained by the Consent Registrar. A subscriber shall also be allowed to view or withdraw his or her consent at any time, for which the access provider shall set up facility for the subscriber to exercise the option to discontinue receiving further commercial communications from that sender, except in the cases which are exempt from the requirement of explicit consent. Consent may also be acquired by an entity other than the one that intends to send the communication communications to the recipients. In such cases, the fact should be clearly indicated while acquiring consent. *Similar provisions are followed in other jurisdictions such as in Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) Act of Federal Trade Commission (FTC) United States of America (USA), for details refer link https://www.ftc.gov/sites/default/files/documents/cases/2007/11/canspam.pdf*

3.3.10 **Inferred consent in cases of prior business or social relationships or in cases of customer's conduct**: Commercial communications may be sent where prior relationship exists between sender and recipient, within the scope of their relationship. The relationship may either be on account of business or commercial reasons, social reasons or it may be because of purchase made by the recipient or transactions entered into between sender and recipient. Such communication may be limited to scope of inferred consent where consent can be reasonably inferred from the customer's conduct or the business and the kind of relationship between the individual and the sender. There may be a wide variety of scenarios where such communications is required to be allowed, which would be too prescriptive to describe in the regulations, so only the broad principle can be defined. However, commercial communications on basis of such relationship should be limited for certain period. **Keeping in view the variety of scenarios, this may not extend beyond twelve months as inferred consent.** Misuse of this provision may be controlled on basis of reports and complaints against entities available in the DL-Complaints, and appropriate action may be taken considering complaints from unique recipients. **In case of inquiry from customer about the product or services, this time period may be shorter and limited only to three months.** Codes of Practice may include further details about requirements for senders to keep certain details in support of such commercial communications and the manner in which these records are to be maintained. CoP may also formulate further specific measure to have better control on UCC in such scenarios. Similar definitions are already being followed in other jurisdictions such as in Spam Act 2003 of Australia Communication and Media Authority (ACMA) for further details refer link *https://www.acma.gov.au/Industry/Marketers/Do-not-call-register/Fax-marketing-standard/do-not-call-register-legislation*

3.3.11 **Templates for Consent and Content to verify content with the scope of consent**: Currently the scope of the consent taken is either too broad or unclear in most cases. In view of this it may be required to specify consent acquisition templates and get them registered. The consent template needs to be presented to the target recipient from whom consent is being acquired. Consent templates would require capturing scope of consent and intent of commercial communications that are to be sent against

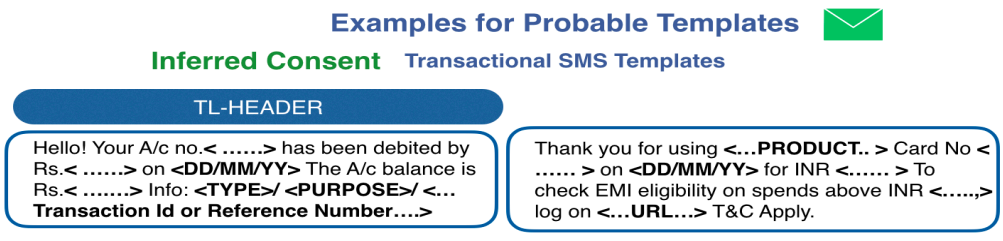



*Figure 5: Probable templates for Transactional Messages*

such consent. Categorization of content needs to be carried out in such a manner that it can be matched to the scope of consent. This may require registration of content templates. There may be multiple templates for consent and content depending upon the situation and the context. Templates may be required to be registered separately for each regional language or combination of multiple languages. There may be separate templates for awareness programs or messages to be sent on the instructions of Government or Statutory bodies and such messages would be considered as service messages. Templates may also be registered for voice calls in form of scripts and transcripts. Honeypots or any special arrangements at the time investigations of complaints may be used to verify the compliance of regulations.

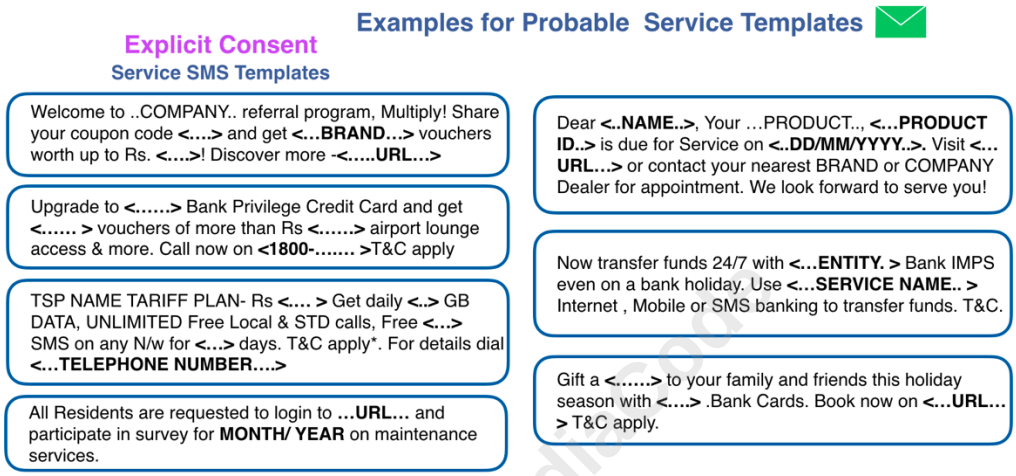



*Figure 6: Probable Templates for Service Messages*

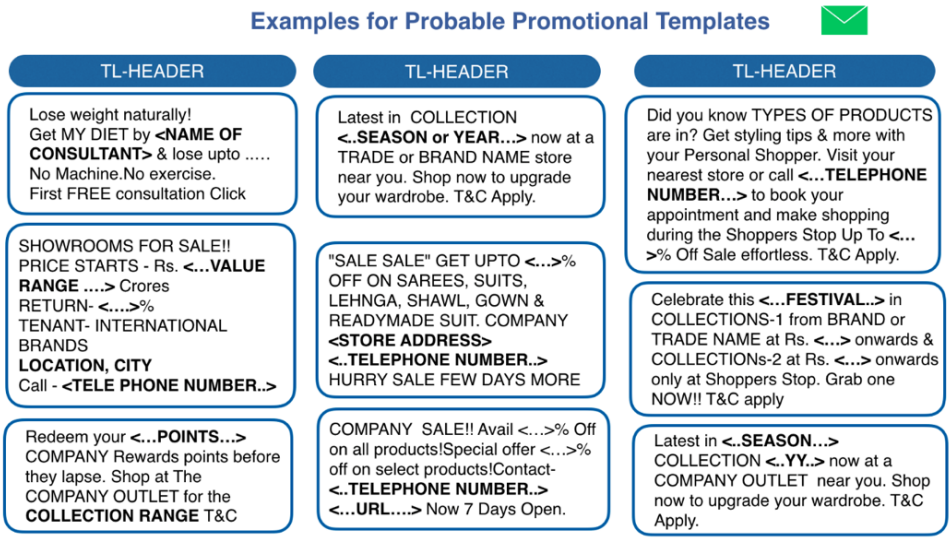



*Figure 7: Probable Templates for Promotional Messages*

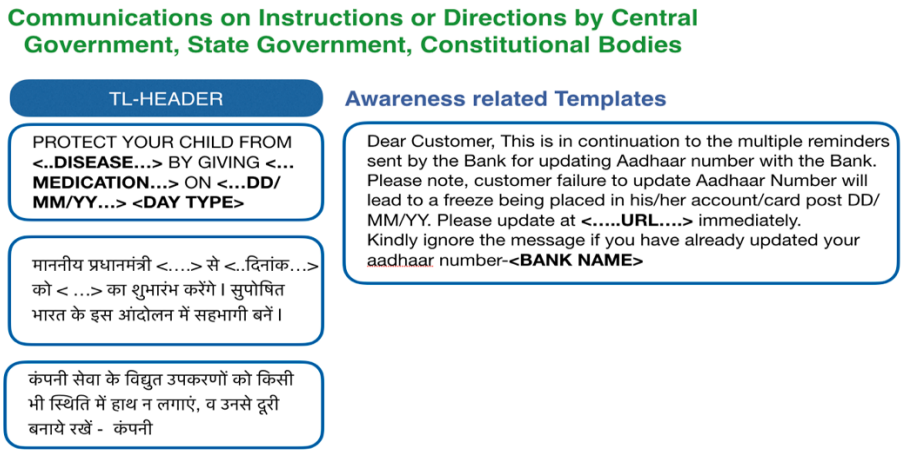



*Figure 8: Probable Templates for Awareness Programs or messages to be delivered on the instructions of Government or Statutory bodies*

3.3.12 Further, to help the recipient identify the type of commercial communications, instead of fixing the format of header for promotional or transactional, it is better to use labels and make them part of content, for example: -

- *Label <Transactional> in case of Transactional Message;*
- *Label <Service> in case of Service Message;*
- *Label <Promotional> in case of Promotional Message;*

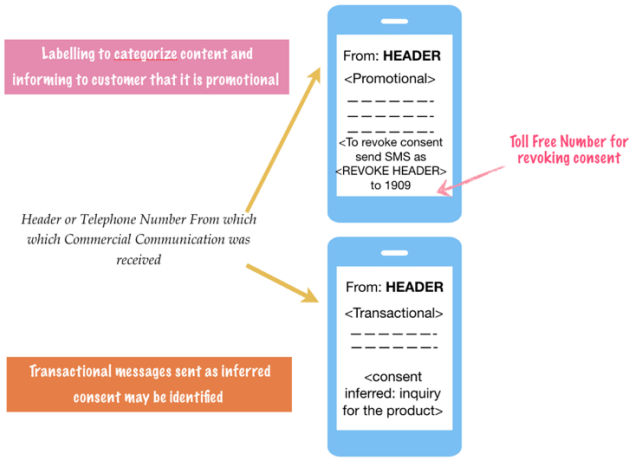



*Figure 9: Labelling of Commercial Communications messages*

3.3.13 In case recipient receives content he or she was not expecting against the consent given to the sender, there would be option to revoke such consent. In case of any gross misuse of consent and content templates, access providers may suspend the consent acquired under disguise or de-register the corresponding content templates. Dispute resolution between participant in UCC eco system and access providers would be in accordance to the agreements in which they have entered into. However, codes of practice may provide further specific details to deal with such situations. In view of the above, the CoP for entities may specify detailed procedure and policies to formulate templates, get them registered and apply them while delivering commercial communications.

3.3.14 **Content templates to avoid instances of misuse on ground of inferred consent:** Consent may be of

explicit type and inferred type. Inferred consent is not explicitly recorded in consent data, and therefore, cannot be checked for in the scrubbing process. However, content of commercial communication sent against inferred consent would largely be against content templates registered for this purpose. To check misuse of provisions for inferred consent, sender may be required to register content templates for sending content against inferred consent. While registering templates, type, nature and length of content may be checked so that it does not contain material for promotional purposes. Post-delivery checks on sample basis, may easily ensure compliance of the provisions for inferred consent. In case of inferred consent, sender may be required to use registered content templates. Further specific details to control UCC in such scenarios would be part of codes of practices formulated by access providers. Codes of Practice would be required to be updated with processes which are more refined considering the complaints and reports received in this regard. Co-regulation approach and provision for Codes of Practices would make UCC eco system to constantly evolve to handle real life scenarios.

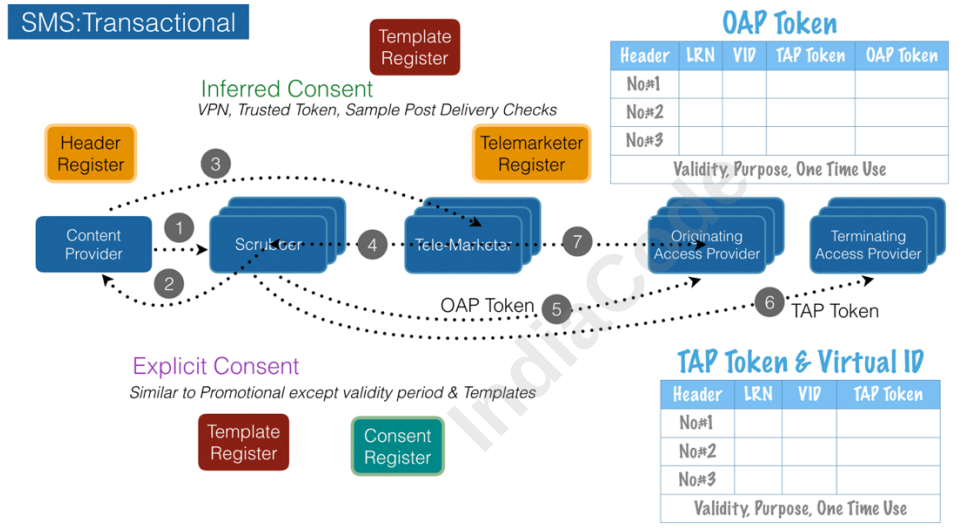



*Figure 10: Illustration of Use of Templates in case of Explicit and Inferred consent*

3.3.15 **Types of Commercial Communications:** Commercial Communications related to transactions may be divided into two types: one, directly related to the transaction where the communication must be immediate or within a short span of time; and the other, related to longer relationship for that transaction. For example, when a person purchases a product or services, a communication may be required to confirm the payment transactions or acknowledge subscription of service, while any follow up message related to expiry of warranty, recall of the product, software version upgrade, etc. may be sent long after it was procured. **First category of communications may be delivered within thirty minutes of the transaction and may be referred to as transactional messages or calls while second type of category of communications may be referred to as the service messages or service call.** Further specific details would be incorporated by the access providers while formulating codes of practice. Commercial communications related to promotions may also be divided on basis of category of content. Using content templates would help to consider content type and scope of consent while delivering and applying pre-checks for regulatory compliances. Artificial Intelligence (AI) and Machine Learning (ML) techniques would help to match the type and category of content being delivered with the interest area of the customer who has exercised option for preference or has given consent. It would also be helpful to design scope of consent in a manner that reflects the type of content under the scope.

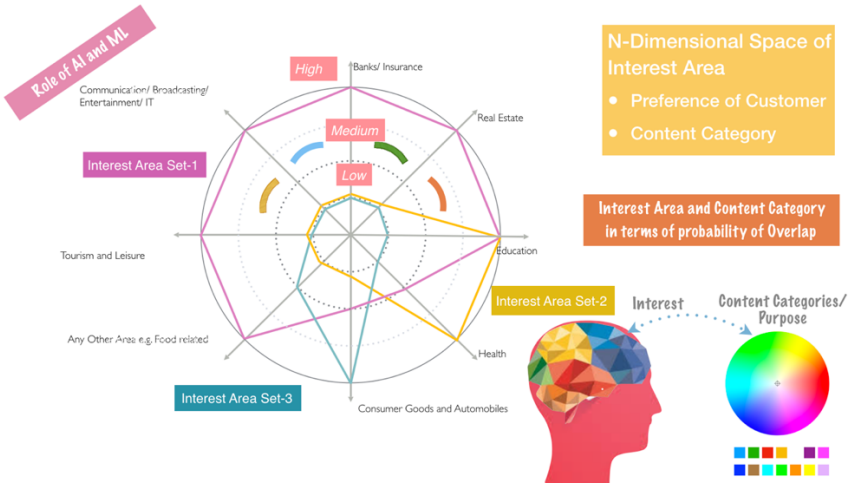



*Figure 11: Illustration for Matching interest area of the customer with category of content*

3.3.16 In view of this, since consent and preferences are closely interlinked, CoP-Preferences should contain details of handling consent. This would include processes for consent recording and revocation, and scrubbing. As with the CoP-Entities, the responsibility of enforcing the codes should lie with the Access Provider, with the regulations only prescribing the regulatory outcomes and objectives.

3.3.17 **Technology driven solutions to enforce provisions in the CoP:** A large number of disparate entities are expected to participate in the system, and such entities are likely to operate from different parts of the country. Senders of commercial communications could be operating for short term or sporadically, or their target recipients may be confined to a geographical area. Regulatory pre-checks and handling data in safe and secure manner requires a large number of processes to be running in sync. Further, these functions may be carried out by different entities in the UCC eco system. If all participating entities are registered and assigned roles and responsibilities in accordance to CoP-Entities, then participants playing different roles would be identifiable and inter-relationship among them would follow protocols to exchange information as defined in the CoP-Entities. Evolution of preferences, scope of consent, operating or interest areas of senders, activity periods or seasons of senders may lead to increase in the varieties of the participants offering services and may also increase the numbers of entities between sender and access provider's network. To bring on board new participants to the system, to control and manage all the participants into the system to follow CoPs, to reconcile records and actions, to act against defaulter and many other such functions requires the adoption of technology driven solutions, without which effective and efficient enforcement of regulations is not possible.

3.3.18 **Technology driven solutions to enable safe and secure data handling as required in the CoPs**: The technology solutions adopted need to address recording of, storing and processing of data, and the execution environments in a distributed environment. Different entities may be involved in one part of the data handling while entities dealing with the other part may be totally different. Data handling may not be limited to administrative boundary of single access provider and may cross administrative domains of multiple access providers. Records of data and records of actions performed by different entities are required to be in an immutable and non-repudiable manner so that participating entities can trust each other. Technology driven solutions providing safe and secure data handling would also encourage principal entities to come on board as they would be more confident about the security of their client data information. It would also boost their confidence in terms of complying with regulations without bearing the risks of non-compliances by other entities. Securing this data would also prevent the data landing in the hands of Unregistered Telemarketers (UTMs). UTMs sending commercial communications would not be able to target customers with particular profile of preferences and may

also be totally unaware about the registration status of the customers. This makes them easily detectable as they would be hitting blindly.

3.3.19 Commercial communications may be pre-checked or post checked, as the case may be, to ensure regulatory compliance. UCC eco system would be built to carry out these checks while protecting preference and consent data even when different entities independently perform certain functions. This would require access providers to develop trusted environment and enroll participating entities to carryout delegated functions in such environments. Availability of Cloud infrastructure and broadband connectivity may offer such possibilities in an easy and fast manner. Virtual identities may also help in carrying out regulatory checks by delegated entities, exchanging information while not exposing the real identities. For illustration, one of the approaches may probably be for sender to submit list of target telephone numbers to a scrubber in a safe and secure manner and for the scrubber to carry out the its function in a trusted environment and while assigning virtual identities to the telephone numbers after scrubbing. Tokens and virtual identities may either be for a complete list or it may be specific to each telephone number in the list. List may also segregate telephone numbers TAP-wise and provide Location Routing Number (LRN) for each telephone number. Virtual identities may be reverse mapped to the real identities either at OAP or at TAP and for this purpose, scrubber may have to exchange information to the concerned OAP or TAP. Reverse mapping at TAP level may provide more security to data by not disclosing real identities to any of intermediaries but it may require special arrangements to route the traffic between OAP and TAP as virtual identities may have digits and characters which may not be routable with exiting routing arrangements. Generating virtual identities or tokens and reverse mapping may also require use of same algorithms at both ends.

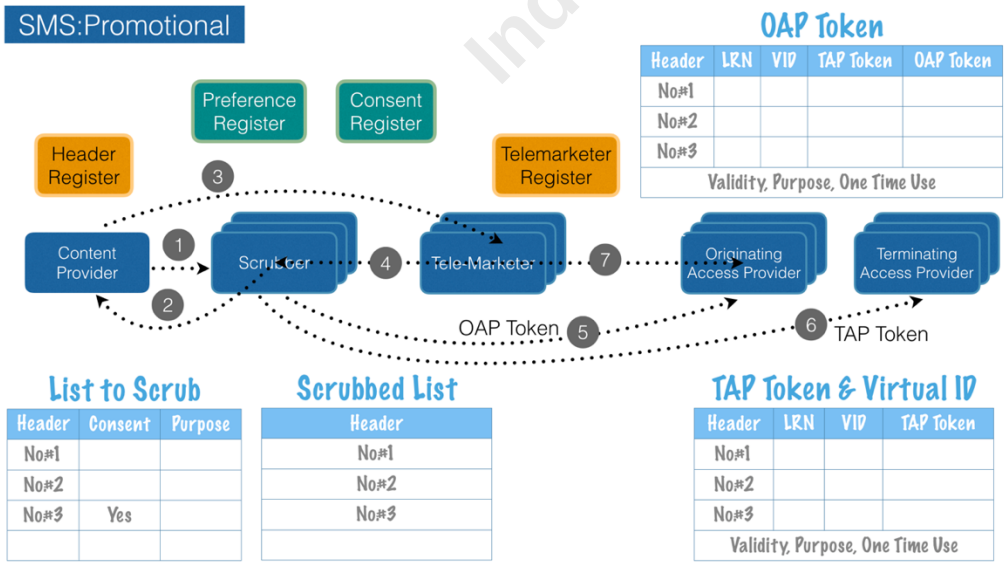



*Figure 12: Illustration for probable approach to protect data while sending promotional SMS*

3.3.20 **Technology to create trust in the system about sender's identity, content categorization and honouring opted preferences or delivering as per the scope of the consent:** Technology solutions which ensures that identity of the sender can be trusted and make him traceable. If the customer is confident that scope of the consent and preferences he has given would be honoured by the UCC eco system, he or she would be more likely to give such consent. This would bring great element of trust and help the UCC ecosystem evolve more around value rather than be a means to block all or most communication. For facilitating TMSEs to make voice calls for justified reasons and legitimate purposes, e.g. alerting and verification by banks in case of high-value transactions, there is need to have separate series or registration of calling numbers which can be presented with name of calling line. Content of

commercial communications via transactional voice calls are also required to be registered as a template of transcript of voice content. For display of name of principal entity in authenticated manner, Calling Name Display, or enhanced CNAME (as per 3GPP specifications) etc. may be used.

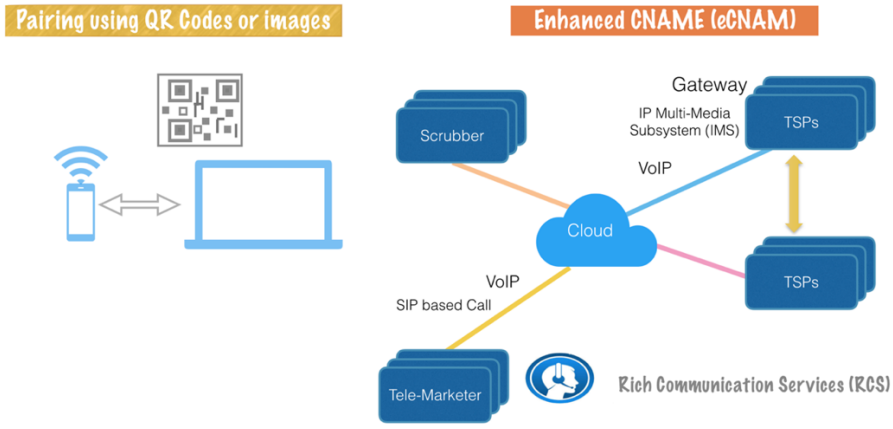



*Figure 13: Illustration for Authentication of Telemarketers during daily operations and displaying authentic name of Sender*

3.3.21 To authenticate the sender or entity of the UCC ecosystem, methods such as device certificates and QR Codes may be used. There may be a mechanism to generate content identity and hash codes using necessary parameters and content which can be applicable for a set of numbers with same content and for defined time interval. Reference templates may be pre-registered with the system and hash codes may be used for verifying that content is according to the template. This mechanism may be helpful for clearly identifying that there is no mixing of transactional and promotional content by the senders. Access Providers must analyse such mechanisms and accordingly include in the Code of Practice.

3.3.22 Laying out processes and assigning responsibilities in the CoPs may not suffice if those processes are not completely followed and defaulters not held accountable. Technology driven solutions would require references in terms of lists of telephone numbers with choices exercised by the customers, reference templates of content and consents for different scenarios to apply requisite checks for regulatory compliance. Different types of Registers and Registrars who are functionally responsible to maintain and provide the requisite functions would be required. Technology driven solutions enabling such functions in the manner prescribed in the CoPs would be required. **Access Providers would implement systems and processes to comply with the codes of practice.** For various function specified in the regulations, it is also required to specify minimum requirements for each registration process (header registration, consent registration etc.) and the functions needed to be performed by the Registrar(s). All such requirements shall be part of Codes of practices.

3.3.23 **Technology Driven Solutions to enable delegating the functions in the CoP to be performed by different entities:** Any or all functions, processes etc. specified in the CoPs may be carried out by the access provider himself or by any other entity, on its behalf. Considering varieties of functions to be carried out that are referred to in Para 3.3.4 of this explanatory memorandum, it is very likely that entities would be interested in performing only specific functions in the UCC eco system. The selected technology therefore has to support unbundling and delegation of functions specified in the CoP to different entities. Sharing of data and execution of process should be in such a manner that process is executed with the data, but it is not accessible in clear text form to any intermediate entity or other applications operating the system. Existence of number of registered entities playing different roles would create a maze of entities where there would be different routes or paths from the sender to access provider's network depending upon choices exercised by the entity to pass on to other entity for

carrying out next function. Paths for same pair of sender and recipient may vary at different point in time and the system has to have the capability to trace the path, as and when required, and identify any defaulting entity. Delegation of functions should be possible without compromising safety and security requirements of the data handling.

3.3.24 **Technology Driven Solutions to provide agility and intelligence to deal with non-compliance:** As deliberated in the consultation paper, the time-gap in resolving complaints is exploited by spammers to continue their activities for longer time span and not acting against defaulting entities in timely manner makes the system ineffective. Proactive approach to control the likely chance of non-compliances would be required to address many issues and concerns raised in the consultation paper. The system chosen would have to have the agility and capability to take quick remedial actions in cases of non-compliance. The system would also have to be smart and intelligent enough to avert any deliberate attempt at bypassing it.

3.3.25 **Core technology complemented by other technologies and solutions:** As discussed in Paras 6 to 10 of this explanatory memorandum, Distributed Ledger technology (DLT) is most promising technology as of now to meet the core requirements referred to in the para(s) above. In fact, DLT is suitable for adoption as regulatory technology (RegTech) for controlling and managing the entire UCC eco system. DLT also provides the capability to implement programmable contracts which can be useful to define business rules as a part of code. The DLT network can record details of entities, headers, consent, content template etc. Distributed Ledger for particular function of access providers may be synchronised with all Distributed Ledgers for same function of all other access providers. It can ensure that all necessary regulatory pre-checks are done for UCC and control is effective and efficient. Considering this, **the Authority has decided that Access Providers should adopt Distributed Ledger Technology (DLT) as Regulatory Technology to develop core of entire UCC eco system, and design solutions around it for meeting the regulatory objectives and requirements of codes of practice.**

IndiaCode

3.3.26 **Complementing Technology Solutions to DLT based core systems:** Core of the UCC eco system alone cannot meet each and every requirement of the UCC eco system. Technology driven solutions which are on peripheries of DLT based core systems would also be required to achieve control and management on end to end basis. Applications on top of DLT based systems may perform functions that meet performance requirements or provide user interface simple enough for all types of end users. All complexities should be absorbed in underlying technologies and intuitive, intelligent, flexible and user-friendly interfaces are required to be provided to the end users. The complementing technology solutions to DLT based core system may include, e.g. APIs, applications, apps, off-DLT execution environments (for specific purposes and cases), Calling Name Display solutions, Artificial Intelligence (AI) & Machine Learning (ML), business reports etc. However, complementing technology solutions are required to meet safety and security requirements and to shore up any vulnerabilities in the system.

3.3.27 **Establishing, operating and maintaining DLT networks:** Access provider would be required to establish, operate and maintain its own DLT networks or may implement it in collaboration with other access providers. In view of above, **the Authority has decided that every Access Provider should develop or cause to develop an ecosystem with the following functions to regulate the delivery of the commercial communications:** -

i. to *provide facility to its customers for registering preference(s) for Commercial Communication and maintain complete and accurate records of preference(s);*

ii. to register entities for participating in the ecosystem and prescribe their roles and

responsibilities for efficient and effective control of commercial communications;

iii. to provide facility to record consent(s) of the customers acquired by the sender(s) for sending Commercial Communication and maintain complete and accurate records of consent(s);

iv. to provide facility for revocation of consent by its customers and accordingly update records of consent for the customers;

v. to register sender(s), carry out verifications of their identities and prescribe processes for sending commercial communications;

vi. to prescribe *process and specific functions of particular entity to carry out pre-delivery checks before sending commercial communications and ensuring regulatory compliance(s);*

vii. to provide facilities for its customers to register complaints against Sender(s) of Commercial Communication and maintain complete and accurate records of status of resolution of complaints;

viii. to examine and investigate complaints, take actions against defaulters and take remedial measures to ensure compliance with the regulations;

ix. to detect, identify *and act against sender(s) of Commercial Communication who are not registered with them;*

x. *to comply with any other directions, guidelines and instructions issued by the Authority in this regard.*

**The Authority further decides that overall UCC ecosystem be developed in such a manner that regulations and code(s) of practice may be enforced. Access Provider(s) may authorise one or more system operator(s), as deemed fit, to provide the DLT solution to all entities, to have effective control over UCC and to keep data secure and safe.** Types of DLT networks are discussed in Para 9 and accordingly recommended networks may be implemented.

3.3.28 **Regulatory Sandbox**: In view of multiple DLT system operators, varieties of complementing technologies, number of probable solution providers and constantly evolving requirements, a test environment may be established (as required) where new functions and processes can be tested, or existing functions or processes can be refined. This test environment may also provide possibilities to explore new ways and means to meet regulatory requirements or new service offerings. Such test environments in regulatory space are commonly known as "Regulatory Sandboxes" and the relevant practices in other jurisdictions have been described in Para 10. Inter-operability of DLT networks with envisaged functions and changes required, if any, to meet the requirements can be identified in this environment. Various stakeholders participating in UCC eco system including principal entities and telemarketers can prototype technology solutions and evaluate processes and functions in the test environment. From regulatory perspective, access providers and other participants would have to be exempt from certain kinds of regulatory action, while they are operating in the sandbox. Since there are uncertainties involved in testing these new solutions, only customer who have given specific consent voluntarily, would be allowed to participate in the test. Mechanism may be required to be developed or measures may be taken to contain the impact within live system, in case, any deviation is observed in behavior of the system or the application under trial from the behavior for which it was intended. For conducting tests scientifically, test protocols and outcome indicators have to be designed and set in advance. During the testing phase, additional steps which may be required to be taken to address regulatory concerns (when the system goes live) may also be identified. Regulatory Sandbox can also be useful to finalize APIs and specific details of implementation. In view of this **the Authority has**

IndiaCode

**decided that it may set up or permit to set up a Regulatory Sandbox for testing implementation of regulatory checks using DLT networks and other technological solutions complementing DLT network(s) and to operationalize such regulatory sandbox, the Authority may, by order or direction, specify the requisite processes.**

3.3.29 **Cost of implementation of UCC ecosystem**: As responsibility of compliance to the regulations would be of access providers and they need to establish systems, operate and manage the DLT based systems, **the Authority decides that access providers be allowed to prescribe fee and collect charges from other participants of the UCC ecosystem.** Charges may be for registration or to carry out activities provided for in these regulations or other participants may also be asked to deposit security with the access provider(s), who may provide for penalties in their contracts for failure to perform the function accepted by other entities.

3.3.30 **Promotional and Service Communication Charges**: Currently RTMs have connectivity with one or multiple TSP(s) referred to as OAP(s) (Originating Access Providers). The telecom network of recipient of commercial communications is referred to as Terminating Access Provider (TAP). Telemarketer may deliver traffic to one or more OAP and OAP may forward traffic to concerned TAP. Primary responsibility of compliance to regulations is of OAP as it is first entry point to the TSP's network (before this point telemarketers may be using Internet or virtual private network). All regulatory compliances may be required to be checked before forwarding traffic to TAP. OAP enters into agreement with the RTMs while providing telecom resources to them. In such situations, OAP should be responsible to ensure regulatory compliance. But when UCC is received by a customer, complaint is made to his subscribed network. TAP is supposed to carry out preliminary examination of the UCC complaint and then forward it to the concerned OAP. While action may be against the defaulter OAP or against the defaulter telemarketer connected to OAP, it is customer of TAP who is affected because of UCC. In such situations, mechanism need to be designed which encourages telemarketers to connect to OAPs who are TAPs for the traffic delivered to them. This would encourage TAP to comply regulation to protect its customers.

InfiCore

3.3.31 In a multiple DLT network systems, there may be requirement to ensure protection of data which is recorded initially by an entity from a particular DLT system while same data might be used by another entity belonging to another DLT system. Appropriate measures are required while such data is shared across DLT systems and for its processing by applications running over DLT systems. It may also happen that an access provider may offer relatively more attractive price and also be lenient in taking action against the defaulters. It would not be desirable to put unnecessary burden on TAP for preliminary examination of UCC complaints which are originated because of poor system implementations by other OAPs or deliberate attempts to capture market by providing protection to telemarketers not complying with the regulations. In such scenarios, it would be preferred to encourage senders to use services of entities participating in the UCC eco system which have direct connectivity with the TAP.

3.3.32 Confining possibilities for all such entities to connect only to TAP would not be advisable as it may monopolize the market and increase the price. To address concerns such as protection of the data, appropriate implementation of system and processes to protect interests of senders and recipients, it may require having structure of promotional and transactional charges that encourages senders to prefer to route traffic directly to TAP and still keep options to take different route if required. In present regulations, promotional and transactional charges are fixed as Rs. 0.05 (five paisa only). The Authority is of view that to discourage traffic from OAPs who is not effectively controlling UCC than other OAPs, these charges may be adopted as ceiling instead of fixed charges. The possibility of saving UCC charges would encourage telemarketers to deliver traffic directly to concerned TAP. However, to discover concerned TAP for a target customer, Location Routing Number (LRN) of the customer may be required

to be fetched. LRN may also be required to be stored in DL-Preferences for complaint handling and for customers who are not registered with any preferences to route reports (information provided by customers not registered about UTMs/ RTMs). Therefore, DLT system are to be designed and established by access providers to query MNP database and if required, keep information in a secure manner. It has been considered that while nature of promotional and service messages is to seek or support the services being provided for commercial gains, the nature of transactional messages is very different and generally it is to inform the customer about vital transactions. Recipient may be required to be Informed in order to protect his interest from any likely misuse or confirm about the transactions or for the purpose of authenticating the transaction. Transactional messages may be required to be sent to comply with other regulatory requirements. Access Providers are getting SMS termination charges for transactional messages as specified by the Authority from time to time. Therefore, there is no need to further compensate access provider for carrying transactional messages.

3.3.33 To allow principal entities to manage their own DSAs, the **Authority is of the view that following measures may be required to be taken**:

i. *assign header or Header root for SMS via Header Registration Functionality, on its own or through its agents, as per allocation and assignment principles and policies, to facilitate content provider or principal entity to get new headers;*

ii. *carry out pre-verifications of documents and credentials submitted by an individual, business entity or legal entity requesting for assigning of the header;*

iii. *bind with a mobile device and mobile number(s), in a secure and safe manner, which shall be used subsequently on regular intervals for logins to the sessions by the header assignee;*

iv. *Carry out additional authentications in case of a request for headers to be issued to SEBI registered brokers or other entities specified by Authority by directions, orders or instructions issued from time to time;*

v. *Carry out additional authentications in case of a request for headers to be issued to government entities, corporate(s) or well-known brands, including specific directions, orders or instructions, if any, issued from time to time by the Authority;*

vi. *Carry out additional checks for look-alike headers which may mislead to a common recipient of commercial communication, it may also include proximity checks, similarity after substring swaps specifically in case of government entities, corporate(s), well-known brands while assigning headers irrespective of current assignments of such headers, and to follow specific directions, orders or instructions, if any, issued from time to time by the Authority;*

3.3.34 Header may be of maximum eleven character or numbers. It may also be a combination of characters and numbers and may not necessarily have maximum length of eleven. Headers may be displayed to the recipient for identifying sender. In case Caller Display Name functionality using Intelligent Networks, ISDN or enhanced Calling Name Functionality (eCNAM) as specified in 3GPP is used, then proper logs and mapping between header and display name is to be maintained by the access provider. In cases of headers, which are purely composed of numbers and same numbers are being used for routing and for displaying identity of calling line to the recipient, then these numbers are to be in line with the National Numbering Plan issued by DoT and guidelines or instructions issued from time to time in this regard. For example, at present 140 series is allocated for telemarketing calls and level 5 is allocated to TSPs for assigning short codes, and level 1 short codes are assigned by DoT. Further details of structure and format of header and levels which are to be considered for assigning to senders would be covered under code of practice.

IndiaCode

3.3.35 **Migration Plan for implementing revised regulatory framework**: Access Provider (s) must prepare a migration plan for the phase-wise transition from the existing system to the new system for header registration, consent registration and other functionalities. While preparing the migration plan, Distributed Ledger (DL) may be introduced by Access Provider or Access Provider (s) for registration of entities (DL-Entities). They will also have to decide the deadline(s) for registering entities with DL-Entities. Provisions need to be made to migrate telemarketer registration module data of NTR to DL-Entities and provide an observer node to TRAI. In view of above **the Authority decides that the Access providers should prepare migration plan for transitioning from the existing data, processes and roles being played by different entities to the new system of data, processes and roles of new entities.** RTMs already registered with the TRAI would be required to register on or before the date of enforcement of relevant regulations in this regard. Migration plan is to be formulated by the access providers and would also include procedures for migration of existing RTMs.

3.3.36 Detailed migration plan would be required to be formulated by access provider(s). This would include identification of typical activities required to be carried out for migrating existing processes and entities into new system and processes. This would also include preparing project management charts detailing sequence of implementation of activities and activities which can be carried out in parallel. On basis of identifying few broad level activities, it is assessed that all requisite activities to implement system and processes envisaged in the new regulations would take 3-4 months from the date of notification of the regulations. Migration plan for consents already recorded by the entities would be included as a part of migration plan for existing entities, processes and data. It may be noted that consent recorded under existing regulations are valid for maximum six months after this time period consent to remain valid after renewing it. Renewal of existing consents and recording of such consents would be required in accordance to the provisions under new regulations. In this way migration of consent would be smooth and spread over time.

InvisCare

## 4 Inputs, analysis and conclusions on issues related to Customer Preference Registration System

### 4.1 Issues related to Customer Preference Registration System: -

4.1.1 **Large time gap between registration or change request and execution for preferences:** The time required for preference registration and its enforcement is seven days and keeping in view, the present technological capabilities, it is too long and is required to be reduced substantially. Reduction in time may require changes in the processes of Provider Customer Preference Register (PCPR), National Customer Preference Register (NCPR) or Customer Preference Database (CPDB) to register preference(s) and update it across all the databases quickly to enforce it. By providing Scrubbing as a Service, telemarketers may not be required to keep their system up for 24X7 and scrubbing would take latest data into consideration and help achieve a reduction in time for enforcement.

4.1.2 **Increase penetration of Mobile App and ensure its availability on devices**: Customers are facing difficulties in registering their preferences as they are not well acquainted with the format of registration of preference. Mobile Apps provide a convenient way to the customer to register his or her preferences. It is required to ensure the availability of Mobile Apps for registering preferences and complaints for all types of devices, OS, and platforms. Penetration of app is required to be increased and it may be done by bundling a white-labelled TRAI Mobile App with other Apps or pre-installing an App with mobile devices. Other initiatives may also be taken for popularizing the app. For feature phone users, a similar type of convenience may be provided by using USSD features.

4.1.3 **Retention of Registration Status during MNP process**: Customers should be able to retain their preferences while porting their numbers. This may require changes in the process for Mobile Number Portability (MNP) and the facility to update the subscription network in the databases of UCC and retain

the status of the customer for preferences.

4.1.4 **Preference Registration in Bulk or by somebody on behalf of him**: Customers may easily register their preferences and change it as and when required if the facility to make registration in bulk for preferences is available and it can be done by somebody on behalf of an organization or family. Introduction of this facility may require changes or defining process and requirement of specific documents.

4.1.5 **More Granularity in choices for Preferences**: It has been reported that many times unregistered telemarketers reach out to customers who have opted out of commercial communications for a given category, but customers are interested in the sub-category of said commercial communication. This indicates that existing categories are too broadly defined, and customers are blocking communications because of it. This also implies that if customers are given more detailed choices of categories, they may be interested in receiving UCC for these specific sub-categories. This requires capturing customers interest into finer categories and also providing options such as acceptable time of day or media type (SMS and/or voice call). Such an implementation would impact processes for CPRF, PCPR, NCPR or CPDB.

4.1.6 **Widening Scope of UCC:** Earlier, some calls and messages were simply annoying, and the concept of Unsolicited commercial communication coined to curb such calls and protect the interest of subscribers, while nowadays, voice call and SMS are also being used by scammers trying to steal the identity or to mislead the target for making some investments. Recently, SEBI and RBI have approached TRAI for help in controlling misuse of UCC channels by unscrupulous elements to send unauthorized investment tips or misguide in some other ways. Tracing of such miscreants is an issue. Sometimes they acquire an SMS header which resembles well-known entities in the market to misguide the recipient into believing that the advice or tips come from experts or authorized sources. Customers frequently report unwanted calls such as silent, obnoxious, threatening calls, Robo Calls, pre-recorded announcements, auto dialer calls and unauthorized communications as Unsolicited Commercial Communications. This indicates that the scope of UCC regulation may need to be expanded, and other Constitutional bodies like SEBI or Government organizations may be required to play a role in curbing such activities. For addressing concerns from Robo Calls and Auto dialer calls, technical solutions are required. Sometimes, such calls originate outside the countries and may require International Co-operation to control.

4.1.7 **Concerns from new types of calls e.g. Silent calls, Robo Calls, Auto Dialer Calls:** Various new types of modes are being used by telemarketers to reach out to the customers and make commercial communications. They are using automated systems to make calls and technological capabilities to reach out to the larger target population. This results in different types of concerns, and customers who earlier did not object to the commercial communications may dislike calls from auto dialers or those with pre-recorded announcements. Steps may be required to address the issues arising from Robo calls and silent calls. Technical solutions to deal with such issue are required and customers may need options to opt out of these new modes. Such commercial communications may also originate from outside, requiring international co-operation and collaboration.

**4.2 Comments of the stakeholders on the issues: -**

4.2.1 **Large time gap between registration request or change and execution for preference:** On the issue of reducing timelines, most of the stakeholders suggested that such reduction is possible. Few stakeholders suggested that this could be done by establishing a central repository for directly registering customer preference through voice or SMS based solution along with a real-time update on the alteration of preference, with the TSPs being simultaneously connected to the central repository. Others have suggested reducing time by providing for instant connectivity between PCPR and NCPR

database through API integration at the operator level. Alternatively, instant connectivity can be established between the operator messaging gateway and the NCPR database, thereby excluding the need to maintain a PCPR database.

i. Many stakeholders supported the idea of creating a cloud-based, centralized and automated platform, to support real-time updates regarding registration/ change/ deregistration of the subscriber preferences.

ii. Moreover, many stakeholders supported that scrubbing as a service will actually reduce the time for enforcement. They recommended that the TSPs & Telemarketers should access the central registry through suitable APIs. One of the registered telemarketers commented that if the RTMs obtain scrubbing as a service from any third party, delays are expected and instead of reducing time, it will increase the time. To address concerns of privacy, one of the solution providers also suggested that the numbers to be scrubbed can be kept in the hashed form and even the screening can be done in such a way that absolutely no information about the numbers is revealed.

iii. Few stakeholders from TSP side mentioned that with increase in granularity, they do not expect significant increase in complexity in operation or in scrubbing. While other stakeholders from TSPs and one from solution provider side submitted that they expect significant increase in complexity and Scrubbing as a Service model would easily handle the increased complexity. One solution provider endorsed the use of cloud computing technology to further reduce the strain on RTMs' capacities and also endorsed prescribing a standard data format such as JSON for RTMs to upload data for scrubbing.

iv. One Stakeholder is not in favour of having scrubbing as a service, however other supported the idea of scrubbing as separate service, but also mentioned that delays cannot be completely eliminated even then.

v. some stakeholders suggested that, from the scaling standpoint, the solutions based on block-chain technology is independent of the underlying architecture which will make it very easy to adopt at any level of the economy.

4.2.2 **Penetration of Mobile App and its availability for all devices**: The stakeholders were almost evenly divided on the issue of bundling a TRAI app that should be supported by all devices and operating systems. While many stakeholders supported such a measure and opined that TRAI should approach the device manufacturers for such default bundling, others opposed on the grounds of it being a forced choice for subscribers, given that other apps existed for the said purpose. Yet others have submitted that the existing mobile apps of access providers should be upgraded to include processes related to UCC. One Stakeholder opposed the bundling on the ground that it would require investment in technology by the regulator.

i. For increasing penetration of app, some stakeholders were of the view that a white-labelled TRAI mobile app may not solve problem, as it will need the regulator to invest in technology and resources to ensure smooth functioning and integration of the app with the current infrastructure stack. This will create unnecessary cost and redundant infrastructure for executing a process that can be more easily performed by the Communication Service Providers, who already have significant penetration with consumers. Further, when all the service providers share a common service for handling UCC, they can also define a common App interface for registering preferences and complaints. This enables developing the App easy for anyone hosting these common services or even a third party. If the UCC services are hosted in the cloud, the cloud service provider can enable the downloading of the app from its portal. The App can also function as an advertising

IndiaCode

platform for the telemarketers and other companies. This can make the app essentially free.

ii. Some stakeholders suggested other initiatives for popularizing this app, like TRAI may advertise this mobile app along with the TSPs who can further educate the customers about the benefit of the app through SMS. TRAI may utilize Proximity marketing/ digital marketing techniques for promoting use and penetration of the Apps.

iii. many stakeholders supported the idea of API based framework which actually makes communications among various stakeholders and parties easy. As a regulator, TRAI should release an API or a kind of a standardized way that could be prescribed that any application which actually seeks to take care of this UCC problem. Some stakeholders had confidence that once industry establishes a standard, the industry will surely come up with the creative solution to enforce compliance.

4.2.3 **Retention of Registration Status during MNP process**: Almost all stakeholders supported the idea of retaining the customer preferences in NCPR as it is i.e. neither de-registering nor re-registering the preferences.

4.2.4 **Preference Registration in Bulk and by somebody on his behalf**: One stakeholder commented to create Digital Customer Profile which can be controlled, accessed and managed by the user.

4.2.5 **Granular choices for Preferences:** Most of the stakeholders supported the introduction of more granularity after a cost-benefit analysis, while some stakeholders opposed it on the ground that it will complicate the process and increase the implementation period.

i. Some stakeholders also argued that additional choices of preferences will impact on CPRF, PCPR, NCPR or CPDB systems and these systems will become more complex and may impact their performance and response time. This may also affect online scrubbing as a service due to overload on the NCPR system. Therefore, the existing system may continue.

ii. One stakeholder suggested that granular preferences would be relatively easier to add for the customer on the app – other avenues like SMS or email mode of registering would be a challenge. High level of specificity in choices can help serve desired objective only when the end to end chain of flow – both SMS or voice calls from UTMs is completely removed.

iii. Stakeholders also stated that the greater granularity will help both customers and telemarketers at the expense of little additional technical work on CPRF, PCPR, NCPR, CPDB, etc. Choices should be in a hierarchical structure of preferences rather than just a long list of options. Customers who prefer simplicity can still fall back on the current method of a single number. Customers who want the refined set of options can go down the tree to specify more precise conditions and preferences. This will also help telemarketers target their messages better to the audiences that are more likely to be receptive. Such targeted messaging will deliver maximum benefit for the resources they spend in telemarketing. One stakeholder suggested that more refined preference registration would give a competitive advantage to the service providers.

4.2.6 **Widening Scope of UCC:** All Stakeholders agreed with the fact that unwanted calls like silent, obnoxious, threatening one are one of the big problems today. Few stakeholders are of the view that TCCCPR regulations pertain only to commercial and transactional related communications. Presently, TSPs use analytical tools based on post-call CDR analysis to curb UCC menace. Using this technique, it is technically not feasible to record and identify missed calls such as silent calls and to proactively segregate A2P & P2P calls into Robo Calls, VoIP calls, obnoxious, threatening calls, etc. Expanding the scope of existing regulations to obnoxious or threatening will impose an unfair financial burden on the TSPs. Such cases may be left to law enforcement agencies to deal with in case to case manner. However,

IndiaCode

other stakeholders suggested that all relevant derivatives of unsolicited communications including silent, obnoxious, threatening calls etc. and unauthorized communications should be captured by the UCC regulations.

i. With regard to the role of the Government in unwanted communications, stakeholders mentioned that the Government should constitute strict laws to mitigate such unwanted communications while simultaneously creating conditions conducive for customers to lodge complaints with local LEA's easily. TRAI can coordinate with other regulatory/enforcement authorities on Threat calls etc., to ensure strict action.

ii. One stakeholder had the view that the standardization of regulations and ownership by government organizations will provide the consumer with the capability to direct its complaints to a centralized authority and will also restrict the unwanted solicitors' capability to manipulate the regulatory norms.

4.2.7 **Concerns from new types of calls e.g. Silent calls, Robo Calls, Auto Dialer Calls:** Some stakeholders were of the view that presently it is not technically possible. As TSPs currently use analytical tools based on post-call CDR, it is technically not feasible to record and identify missed calls such as silent calls and to proactively segregate A2P & P2P calls into Robo calls, VoIP calls, obnoxious, threatening calls, etc.

i. However, other stakeholders have suggested following technical solution to fight back such UCC: (a) Telecom providers can also use the call duration – silent calls originate with a barely 1 second long missed call which is an extremely rare case from a customer to customer calling context; (b) Signature solutions (pattern detection) and Honeypots to be deployed by telecom providers, designed specifically for robot/silent calls – License cancellation upon non-compliance should be mandated; (c) In the US, there is a technical approach being considered which when deployed, with various other mitigation techniques like honeypots, Black-list/white-list etc., should provide a layer of authentication and verification that would put trust back into the network and enable rapid and efficient trace-back for investigation and enforcement purposes.

ii. Stakeholders also informed that the Federal Trade Commission and local industry bodies explored various approaches to stem Robo calling and spoofing. They determined that major changes to the legacy SS7 signaling protocol prevalent in voice network infrastructure was not viable and has thus focused the solution on next generation IP Multimedia Subsystem (IMS) network interconnection. To be clear, the approach does not require all voice switches to migrate to VoIP, only that the interconnecting trunks between operator networks employ IMS-based VoIP. Furthermore, SMS text messaging generally uses other signaling protocols for Application to Person (A2P) messaging which would require a comparable IP-based approach unless IMS is also adopted for such messaging to consumers.

iii. One Stakeholder suggested that the registration and authentication process of the new framework should ensure that calls can be made only from some registered numbers. The validation process of the new framework may also ensure that the format of the message/calls is approved before distribution. This would considerably help in curbing Robo calls and silent calls.

iv. Regarding International co-operation and collaboration needed to address the issues, no specific comments were received from stakeholders.

### 4.3 Analysis of inputs and conclusions

Following paras deliberate upon the issues which are related to Customer Preference Registration System (CPRS). Issues and responses to the questions raised in the consultation paper are also summarized. Key points from the current regulatory approach and approaches taken in other jurisdictions to deal with the issues were

indiaCode

also considered while analyzing inputs and concluding the issues. Analysis of inputs and conclusions of the Authority are as follows:

4.3.1 **Reduction in time for registration and its enforcement**: Currently time gap between registering preferences and its enforcement is seven days and it is due to spread-sheet-based implementation and updating databases via running scripts in episodic manner. This time gap can be reduced by adopting technology-based solutions. For this, automation of processes and use of APIs to update databases would be required. For reduction in time to enforce the registered preferences, Scrubbing as a Service would enable the function of scrubbing to be performed by any registered entity, providing flexibility to Telecom Service Providers (TSPs) and RTMs and easing them to maintain the requisite hardware. In view of above, the **Authority decides that request of preference registration, de registration or modification should be done within 15 minutes and recommends that revised preferences be enforced within a time period of twenty-four hours from the time of registering preference or changes to it**.

4.3.2 Customer Preference Registration Facility (CPRF) should be available on multiple modes of communication as being provided under the current regulations. USSD may also be provided as an additional mode as it may provide interactive way for feature phone users to register or modify preferences. Web portal may be very helpful to provide interface to manage preferences and the customer may be authenticated via OTP. Web interface may also assist feature phone users and also provides options to take help of family member or friends to set preferences on the customer's behalf. As penetration of mobile Internet is increasing at fast pace, mobile App may further be enhanced to provide internet-based interaction with the system in addition to the other method.

4.3.3 It is observed that if customer has attempted to register or manage preferences, but the request is not exactly in the same format prescribed in the regulations or information is inadequate then requests are being rejected and if customer is not aware at that point in time, exactly what changes are required in the submitted format then gets unsatisfied with the CPRF. The Authority is of the view that access provider should not simply reject the request but help or guide the customer to do it in right manner next time. For this purpose, one of the way may be to provide information to the customer to download and use mobile app which takes care of format related issue. In view of above, **the Authority decides that access provider be required to provide details about format and procedure to customer whose request has been rejected on grounds of incomplete information or incorrect format and codify this requirement in the appropriate Code(s) of Practice**.

4.3.4 **Adopting technology driven solutions**: Distributed Ledger Technologies (DLT) (refer para 6 to 10 of this explanatory memorandum) with complementing technology and platforms can enable sharing of preference data and execution of scrubbing processes, in a multi participant environment, in safe and secure manner. Authority is of the view that technology driven solutions may take care of complexity for providing refined choices of preferences and quickly applying for enforcement while end users of the system may need to deal only with the business interfaces. The technology will also make it easier to implement the proposed 'Scrubbing as a Service' model.

4.3.5 Preferences should be recorded on the Distributed Ledger for Preferences (DL-Preferences) and be made available for scrubbing. DL-Preferences should be established, maintained and operated by the access provider or any other agency on its behalf. DL-Preference ledger should perform following functions:

i. *recording preferences of customer(s) in non-repudiable and immutable manner;*

ii. *maintaining relevant details about customer;*

iii. *retaining preferences information during mobile number portability process, with changes in*

India Code

*Location Routing Number (LRN) of the new serving network, in case customer is being ported-in;*

iv. *creating a new entry, during subscription opening process, for starting life cycle of a phone number with new subscription;*

v. *recording subscription closing, for completing the life cycle of a phone number with current subscription;*

vi. *synchronizing it with DL-Preferences of all other access providers, in real-time;*

vii. *providing an observer node of DL-Preferences to TRAI, or any agency authorized by Authority, free of charge;*

viii. *recording revocation request for consent on Distributed Ledger of Consent Register as prescribed;*

4.3.6 For recording preferences on Distributed Ledger for Preferences (DL-Preferences), Access Provider shall automate its internal systems and develop appropriate APIs to interact with DL-Preferences;

4.3.7 More granularity of choices in the preferences for selecting a category of commercial communication may help the customer indicate his interest areas in more precise manner. Having granular control on the topic and content of UCC is likely to increase the chances of customers signing up for it (or rather not blocking it). This will benefit both customers and telemarketers. Customers benefit from having access to communication of their choice, and telemarketers will benefit by having better targeting. Initially, exercising choice in great detail and considering them while sending commercial communications may seem complex, but using enabling technologies, such as intelligent, multi touch interfaces, web interfaces, assisted mode to set preferences, platform approach (API's to set, change or revoke) can allow innovation in the market to find the best solutions.

4.3.8 Granularity in the preferences may be introduced either by creating more categories or introducing multiple levels in hierarchical form. Requirement of granularity is expected to constantly evolve and pre-deciding particular categories or sub-categories in comprehensive manner is not practical. In view of this, **the Authority decides that regulations should enable TSPs to create more categories and more types of preferences e.g. modes, time bands, day types in evolving manner. The details of categories should be specified in the part of Code of Practice for Preferences (CoP-Preferences) which is to be formulated by the access provider(s). Expansion of categories or sub-categories should be in such a manner that customer whose preferences are already registered are not altered without their consent.**

4.3.9 Introducing more dimensions to the preferences like time bands, types of day, medium of communication etc. would make available more options to the customers who may be interested in communication with certain preferences in terms of time or day or ways sender may reach out to him. Not providing such options to the customers may lead to opt for fully blocked state while he was not averse for all such commercial communications. Such a situation, is exploited by the UTMs as it would be possible to strike a deal if they hit blindly but by chance they fit into the narrow requirements of the customer. This situation may make success of UTMs overweigh risks of stringent actions taken against them. Introduction of additional dimensions may initially seem complex and difficult but default options in case detailed options are not exercised by the customer may keep customers at same level as of not having additional dimensions and there won't be any adverse impact. Technologies, solutions and innovative user interfaces have to take care of all underlying complexities and offer such options to the customer in a user friendly, convenient and simple to use manner. Agile and flexible ways to evolve such preferences over time would make system adaptable to customers behaviour.

4.3.10 The Authority has noted that Mobile Apps have played an important role in providing customers a

TRAI Code

convenient way to register, de register, modify and view preferences. Apps can make it easier to allow management of additional dimensions of preferences and changing theses preferences frequently and registering them in a short time. **The Authority decides that all access providers shall ensure that all devices registered on its network support permissions required for the functioning of apps developed in this regard either by the Authority or any other person or entity and approved by the Authority.**

4.3.11 It is being observed that there was no process specified to deal with the preference registration status of the customer while porting the number. This is causing inconvenience to customers, because their preferences are either changed or completely reset. Similarly, no process is defined to deal with the situation when telephone number changes ownership and the preferences of the new owner need to be reflected in the records. In view of this, **the Authority decides that during MNP process, the preference status should be retained and current Location Routing Number (LRN) may also be recorded on DL-Preferences**. DL-Preferences must also keep other details, e.g., phone number in international format, lifetime history of preference registration, modification and de-registration with date(s) and timestamp(s), unique registration number issued at the time of registration of preference. Records of consent corresponding to number would be retained in DL-Consent for a certain period and in a certain way as specified in codes of practice. It would be helpful to attribute UCC complaints and reports against such number or UCC related complaints or reports made by such number.

4.3.12 Regarding issue of bulk registration, it was noted that preferences should be managed only with the permission of the customer and option of bulk registration by representative may not be required. However, if the customer wants to take help of others who are acquainted with the process or have access to better user interface or device capabilities e.g. mobile app, web portal, multi touch screen then assistance to manage preferences may be taken or other devices may be used while managing the preferences. In view of above, **the Authority decides that option to manage preference using other's telephone numbers or using web interfaces may be provided but request should be authenticated through OTP sent to the customer**.

4.3.13 Communications from Political Parties related to political campaign and from entities sending communications to survey the market may not be directly falling under the definition of commercial communications. However, some customers may experience inconvenience or irritation or annoyance as in case of UCC. Regulatory framework for UCC which provides capabilities to record consent and set preferences, may be very useful to provide options to customers to set their preferences to opt out of such types of calls or give consent to such entities to send such communications to the recipients. However, this may require further consultations with the concerned Government bodies before taking a position in this regard.

4.3.14 It is noted that there are serious concerns of customers receiving fraudulent communications, obnoxious communications, threatening calls and malicious calls which are not as such unsolicited commercial communications (UCC). Customers may be given options to report such incidences to the concerned authorities, who are willing to participate in the system and take remedial actions. **The Authority is of view that dealing with such issues is not under the purview of the TRAI but UCC eco system may be designed to pass on such information to concerned authorities, organizations or entities if such entities are willing to participate in the eco system.** For example, lottery, renting offers for installing mobile towers, seeking personal information, investment tips or advisories from unauthorized sources using voice call or SMS can be routed to concerned participating entity such as SEBI, RBI, Associations in the sector etc. **The Authority decides that scope of UCC should not be widened but UCC ecosystem may enable for participation of interested government bodies or constitutional bodies or associations recognized by the authorities in the concerned sector.** Moreover, UCC eco system should be able to provide information on the identity of the sender and

IndiaCode

associated information about it.

4.3.15 Robo Calls, Auto Dialers with pre-recorded announcements and Auto dialers with live agents are a new source of UCC. These systems are sometimes causing spurt in UCC, repetitive call attempts to same customer in short span of time and also leading to silent calls which is very annoying to customers. These calls are difficult to proactively detect such callers but there must be regulatory provision to deal with the situation when it comes to the notice of the access provider or to the Authority. For senders who are registered and want to use Auto Dialers and the recipient has no issue in receiving such calls, it may be permissible. However, differences in volume of calls originated by the auto dialer and capacity of the system to handle answered calls may lead to abandoned calls. Auto dialers may also lead to silent calls because of its improper functioning or may be deliberately misused to make commercial communications in a disguised manner. In cases of complaints against UCC, normal procedure is to verify occurrence of communication by verifying call detail records, which may be misleading in cases of return calls to missed calls where call logs may suggest that the communication originated from the customer's side. Auto dialer may also lead to abandoning of calls due to paucity of human resources available at particular moment to deal with answered calls. **The Authority decides that no sender registered for making commercial communication should initiate calls with an Auto dialer that may result in silent or abandoned calls. Further, the sender must notify the originating access provider, if auto dialer is being used to make commercial communication and taken steps to maintain abandoned calls within the limits provided for in these regulations or Code(s) of Practice.** Regarding Robo calls, it is required to collect more information about the character and incidences of such Calls and take action take at the appropriate time.

4.3.16 Issues and concerns from Auto Dialler calls have been noticed in other jurisdictions as well. For example, telecom regulator OFCOM and Information Commissioner's Office (ICO) from United Kingdom (UK) and Federal Trade Commission (FTC) from United States of Americas (USA) have provisions to take actions to control nuisance from auto dialler calls. Use of Auto dialler by UTMs may come into notice via complaints and reports from the customers. Inputs from honeypots and usage patterns from the telephone number(s) may be analyzed to investigate the reported use of auto dialler. In case, it is found that auto dialler are being used by UTMs then appropriate actions may be taken against such activities. In case, auto dialler are to be used by Senders of commercial communications then they have to give prior intimations to the access providers. Senders using auto dialler have to follow certain performance requirements for auto dialler such as percentage of silent calls, percentage of abandoned calls etc. to be within specified limits. Access providers may cross verify performances by analyzing statistics of usage pattern of telecom resources being used for auto dialler. Further specific details would be included in the codes of practice (CoP) which are to be formulated by the access provider(s). For curbing menace of UCC from Robo Calls, available options for implementation may be required to be explored. Industry may also develop new solutions for ways and means to control UCC from Robo calls. **The Authority may permit or set up regulatory sandbox for conducting tests on proposed solutions for Robo Calls.**

4.3.17 Considering that in the proposed system, UCC preferences and the approaches to register them are expected to evolve over time, **the Authority is of opinion that co-regulation would be the best way forward. Accordingly, access providers will be required to formulate Code of Practice for Preferences (CoP-Preferences) and submit to the Authority. This CoP will include processes for handling all aspects of managing preferences and consents including revocation of consents. Once CoP is formulated and finalized, access provider will be required to abide by its provisions. The Authority may intervene and issue directions or orders to modify the CoP, if it finds any deficiency in the CoP or it finds that CoP is failing to serve the purpose. The Authority may also formulate standard CoP, if required.**

IndiaCode

## 5 Inputs, analysis and conclusions on issues related to Complaint handling system

### 5.1 Issues related to Complaint handling system

5.1.1 **Large time gap between registration and resolution of complaints:** Current process for resolution of complaints are time consuming and the time gap between detection of violation and enforcement action is exploited by the spammers. Gap in time between UCC complaint and its resolution needs to be reduced but extent of reduction may depend upon automation of the process and require changes in the functions and interfaces for the complaint handling system.

5.1.2 **Changes in Complaint Registration facility to improve complaint registration**: Consumer Complaint resource facility (CCRF) may need to be provided in a manner that improves the success rate in complaint resolution process. If pre-validation of data, e.g. by using Mobile App, web portal is done during registration of complaints, the success rate of the complaint resolution process could be improved.

5.1.3 **Entertaining complaints from customers, who have not registered any preference**: Complaints may be made by customers who have not registered with NCPR but who receive commercial communications in violation of the provisions of the regulations, e.g. communications beyond specified timings. Mechanisms may also be explored to avoid promotional commercial communication during roaming or in cases when calls are forwarded.

5.1.4 **Make available intelligent Mobile App on all devices for UCC registering complaints:** TRAI has developed a Mobile App which can be used to file complaints. Such mobile apps may be further developed and enhanced to make them more intelligent and intuitive for submitting UCC complaints. These mobile apps would be required to be available on different types of mobile devices and operating systems. It may be necessary to mandate device manufacturers, Operating System developers and platforms to allow the apps to have the requisite permissions for proper functioning.

5.1.5 **Reviewing structure of financial Disincentives for Access Providers**: Present provision of Fianancial Disincentives for Access Providers may need to be reviewed and additional roles and responsibilities may be assigned to Access Providers. Additional measures may be prescribed for the access providers to mitigate UCC problem.

5.1.6 **Levying stringent Financial disincentives in case of UCC calls using Auto diallers, Robos etc.:** Customer should have the option of opting out of commercial communication delivered through new modes such as Robocalls and auto-dialler calls. There should be strict financial disincentives for telemarketers sending UCC in violation of regulations using Robocalls or auto-dialler calls.

5.1.7 **Enhancements of Signature Solutions**: Signature solutions may be enhanced to identify unregistered telemarketing activity. Technology based detection solutions which can proactively identify suspicious activity, need to be developed. Inputs to signature solution may come from various sources, e.g. by deploying honeypots or network elements. Enhancements of signature solutions may also include sharing of information among access providers for continuous evolution of signatures, rules and criteria.

5.1.8 **Use of Artificial Intelligence (AI) to improve Signature Solutions**: Artificial Intelligence (AI) may be useful to improve performance of signature solutions and make it more adaptive to changes in the behaviour of and techniques used by the telemarketers to bypass the signature solution. AI may also be helpful to detect newer UCC messages created by tweaking content.

5.1.9 **Honeypots to detect UCC and collect evidence**: Honeypots may be used to detect and collect evidence for UCC, which may be difficult to capture otherwise. Approach for deploying such Honeypots may be required to be developed.

Draft Code

5.1.10 **Crowdsourcing of information to detect UCC**: Developing Intelligence through crowdsourcing by analysing UCC complaints at central locations may help in identifying source of spam and expediting actions against such defaulters.

5.1.11 **Scrubbing as a Service**: Scrubbing as a Service model, as discussed earlier in para 3 and para 4 would be useful to handle complexities of more categories and dimensions of preferences, to consider consents while scrubbing and reduce time to enforce changes in the preferences. From complaint handling perspective, past logs of scrubbing activities need to be available which are immutable and non-repudiable. These logs need to be available in a manner which reduces complaint handling time. Scrubbing as a Service may be chargeable and models for charging may be different based on requirements and/or volume of communication.

5.1.12 **Mitigate or eliminate victimization**: Aggressive actions aimed at suspected unregistered telemarketers may sometime lead to victimization of customers, on account of false or faulty complaints or due to misidentification. The complaint handling mechanism has to be able to prevent or mitigate such victimization. There need to be processes for determining whether the owner of the number against whom a complaint has been filed has a business or commercial relationship with the complainant. Instead of disconnecting telecom resources immediately, there need to be provisions to issue notices, to put connections in suspend mode, and to put Usage Cap till investigations are completed.

5.1.13 **Developing Scoring System for detecting UCC**: It has reported that unregistered telemarketers often take SIMs from multiple access providers and changes their patterns in order to bypass detection. To detect and act against such UTMs operating across service providers or RTMs involved in unauthorized activities, a scoring system needs to be developed. Data from this scoring system can be shared access providers to further enhance their signature solutions. Parameters which should be considered for determining the score need to be identified and agreed upon by access providers.

Indiacode

**5.2 Comments of Stakeholders**

5.2.1 **Reduction in time gap for complaint resolution**:

i. Regarding automation of complaint handling system (Real time/cloud based), most of the stakeholders agreed that there is a need to reduce the delays but practically doing it may be a challenge. Stakeholders submitted that, current system require 7 days Turn Around Time (TAT) in total (3 days for OSP & 3 days for TSP & one day for close looping). There is scope of compressing the Turn Around Time (TAT) by 1 day each side (excluding Saturday & Sunday), but **2 days are required for proper validation of CDRs**, due to customer data privacy the CDR access is available only with Nodal officer of circle. Moreover, at times TSPs have to co-ordinate with RTMs for locating activity logs.

ii. Few stakeholders stated that most of the TSPs are already using semi-automated or automated process for receiving complaints and for its resolution, it includes complaint logging through self-service mode like SMS, web, mobile App. **They can further automate** it, **by applying additional validations** at initial level of examination of complaints such as registration status of the customer, length of UCC content, length of header, key word filtration of content etc., and can **instantly provide the reasons for rejection of invalid UCC complaints** to the complainant.

iii. One stakeholder suggested that a possible change can be the **early barring of telecom resources allocated to a UTM** post an advance notice and an opportunity of being heard. The outgoing services should be barred immediately on validation of the complaint with the CDRs and notice of disconnection should be issued to the customer. Telecom resources **should be disconnected if no reasonable and admissible justification is received within 3-4 days**. In the meantime, the complaint may be closed on the basis of applying barring of usage of telecom resources. UTM

details should not be published on the NCPR for blacklisting till a final decision is taken on unbarring or disconnection.

iv. Many stakeholders supported the idea of using centralized cloud-based complaint redressal system. During OHD, some stakeholders suggested that it is technically possible to maintain **all complaint related information through either a centralized database or through blockchain technology**. Using this system, as soon as, a complaint is registered it should be also possible to track the history of a UCC call or SMS, its content and whether it should have been sent in the first place.

5.2.2 **Changes in Complaint registration facility to improve complaint resolution**

i. All the stakeholders agreed that structured and pre-validated inputs from complaints using Mobile Apps and web portals may be helpful to capture relevant details of complaints, to automate resolution and enable advanced post-facto analysis for accurate reporting. App can have the built-in functionality of capturing call/SMS records from specific set of numbers – 140 series, SMS headers etc. for accurate data analytics, predictive modelling etc.

ii. Other suggestions were, to extend CRM-like functionality for purpose of registering complaints and make it a self-service functionality and may also provide **Chat-bot functionality** on the Web Portal.

5.2.3 **Entertaining complaints from customers who have not registered any preference**

i. TSPs and Telemarketers are of view that **UCC complaint registration for non-DND customers should not be allowed**, as this will create junk in the complaint database which will delay the resolution of complaints made by DND registered customers. Such customers should be **encouraged to register their preference in the NCPR before lodging complaints**. This will be one mode to popularise the exercise of preference by customers. Other stakeholders supported the view that access providers should provide resolution to customer complaints from customers who are not registered with NCPR, on the grounds that this **will help access provider identify UTMs and RTMs which are not complying with regulations**. Few stakeholders suggested that dynamic registration can be provided for customers not registered with NCPR.

ii. Regarding the mechanism to avoid promotional call or SMS during roaming/call forwarding cases, Stakeholders suggested the followings:

a. Few stakeholders suggested that customers may be provided with an option to opt-out to receive promotional commercial communication during roaming or call forwarding. TAPs may complete promotional and non-critical transactional communications only when customer is within his home service area. Filtering mechanisms may be enabled at intermediate nodes to detect promotional communications and modify headers to prevent additional forwarding in the system.

b. Other stakeholders submitted that it would be difficult to implement it as there would be no difference in the calls to a customer who is in home service area with respect to the calls to a customer who is roaming. Calling Line Identity (CLI) would be same in both the cases as far as the call is coming from a registered telemarketer with a registered CLI which has been assigned for the purpose.

5.2.4 **Developing and enhancing mobile App for all device OS**

i. Almost all stakeholders were in agreement for the need to develop and enhance the mobile App which would be helpful to submit complaints in an intelligent and intuitive manner. They were also in agreement to make it available for all device OS. However, they were of the view that

InfraCode

TRAI may issue necessary directions to device manufacturers for ensuring proper functioning of operating systems or platforms which are available to TRAI's UCC mobile app.

ii. While one stakeholder suggested that TRAI mobile app should be promoted by all service providers/manufacturers & software providers. All permissions required by the app should be available on the phone by default. Customer may have option to modify. Mobile app makes it easy to manage preferences/ consent and complaints. App can also make it possible to run data analytics to further improve processes.

5.2.5 **Review of structure of financial disincentive for access providers**

i. Stakeholders from the side of TSPs have a common view that there should not be any provision of the financial disincentive on the TSPs unless there is any violation at TSP end with regards to any regulation/direction issued by the Authority from time to time. The financial disincentive imposed on Access Service providers on account of UTM should be done away with. Few stakeholders suggested that present system may continue, and access providers may further strengthen process to be followed at the time of providing telecom resources to RTM, TMSE, aggregators etc. They may also consider including location tagging of place of office premises / place from where commercial communication calls would be made. TSPs also submitted that they do due diligence at the time of providing telecom resources and also carry out appropriate checks and they should not be held responsible for any violations by UTMs. TSPs further submitted that for management of header, TMSEs should be responsible and not the TSPs. It was also submitted that TMSEs should be made liable for appropriate use of headers and responsibility should be made clear at the time of assignment of header. **TSPs should not be made responsible for any misuse of headers.** TSPs requested Authority to **remove provisions of financial disincentives on access providers in case of violations by UTMs**.

ii. Few TSPs submitted that they take several actions to identify UTMs such as analyzing calling patterns, their locations. TSPs have implemented spam detection solutions and they regularly update scripts for better results.

5.2.6 **Levying strict financial disincentives for UCC using Robo call, auto-dialer calls**

i. Few stakeholders suggested to institute an automated screening system for filtering robocalls. They also suggested use of honeypots to identify such calls. In case, it is found after an investigation or it is evident that entity is making robocalls or using auto-diallers for telemarketing purpose then TSPs may be directed to disconnect the telecom resources of such callers. Further, if such calls are generated through RTM, a suitable penal clause in the agreement may be incorporated and such RTM should be blacklisted with immediate effect for a longer period beyond three years along with immediate forfeiture of Security Deposit. This shall act as a deterrent to RTMs from indulging in such activity.

ii. Other stakeholders submitted that there is **no mechanism available in the industry to proactively identify the nature of calls/ SMS**. Since TSPs have no control over those customers who are making calls or sending UCC spam, therefore **TSPs should not be unduly penalized for inappropriate action of customer**. The strict financial disinvestment should be applied on the TSPs only when there is violation of the Regulation and not on the basis of such UCC calls being generated in their networks. Stakeholders also submitted that, in some cases, a Robo call may be a legitimate call from a doctor's office reminding a patient of a crucial appointment.

5.2.7 **Enhancements of signature solutions**

i. Some stakeholders recommended use of machine-learning and information sharing among

Indiacode

access providers to enhance the signature solutions. New patterns detected or learned by one Access Provider may be immediately adopted by other Access Providers. They also suggested to use e-signatures and hash-codes and recommended creating a centralised data sharing and coordination platform to facilitate this.

ii. Other stakeholders did not support enhancing existing signature solutions.

5.2.8 **Artificial Intelligence (AI) to improve performance of signature solutions:** Most of the stakeholders agreed that Artificial Intelligence (AI) based solutions can improve the performance of signature solutions and enhance its capabilities. For example, AI with honeypot can have an artificially intelligent bot which can be programmed to interact with suspected unregistered telemarketers or registered telemarketer not complying with the regulations. Such measures can also help to learn emerging new patterns in UCC which may be required additional remedial measures to be taken by the access providers. These patterns than can be shared with the various TSPs for the implementation in their signature solution. Stakeholders submitted that implementation of the AI solutions would require more discussion between TRAI, TSPs, and vendors.

5.2.9 **Honeypots to detect and collect evidences for UCC**

i. TSPs agreed that honeypots can be helpful in detecting and collecting evidence of unsolicited communications. An artificially intelligent honeypot can be programmed by TSPs to fish out defaulter telemarketers/ UTMs on the basis of call patterns. However, only new numbers should be used in honeypot i.e. no recycled number should be used in honeypot, as it may be possible to get solicited communication on such numbers. Stakeholders also suggested that deployment of honeypots along with use of cryptographic signatures to collect evidence can help to identify similarity among samples collected from multiple sources. Such measures can also make use of additional software capabilities such as to detect plagiarism/ to detect similar image/music, that can help to identify similarity among samples.

ii. Few stakeholders have suggested to identify the entity who should be responsible to deploy Honeypots, analyse and deal with inputs from such Honeypots.

5.2.10 **Crowdsourcing information to detect UCC**

i. Most of the Stakeholders supported the view that complaint related data should be analysed at central locations such as TRAI's NCPR Portal to develop intelligence, take proactive measures and to strengthen the system in a structured way.

ii. Inputs may be shared with all stakeholders and actions against identified defaulters may also be expedited.

5.2.11 **Scrubbing as a Service**

i. Comments of stakeholders on Scrubbing as a service model related to entity registration and preference or consent related requirements are already covered under para 3 and para 4.

ii. Stakeholders suggested that charging for scrubbing as a service may be based on categories or volume. Minimum charges may be applicable for carrying out scrubbing or there may be one-time charge (akin to registration fees).

5.2.12 **Mitigation or elimination of cases of victimization**

i. Most of the Stakeholders were in agreement for the need to have mechanism which avoids or eliminates victimization and supported options such as Reputation-based analysis which may take into account various factors like age of subscription, authentication at the time of subscription, address verification method etc.

India Code

ii. Some of the stakeholders also supported need of considering complainant's prior business, commercial or social relationship with the party against whom complaint is made need to be considered while resolving the complaint. They also submitted that TAP need to have access to a database of customers mapped to their business/commercial relationships so that potential cases of false complaint may be flagged before sharing with OAP. The actual process of registration may also be enhanced to record the source, timestamp and additional relevant metadata like parent-child, peer or family-based relationships that may be relevant in dispute resolutions.

iii. Stakeholders suggested that first notice should be issued then connection may be put in suspend mode or applying Usage Cap till investigation is completed.

5.2.13 **Developing a scoring system for UCC**

i. TSPs are of view that present signature filtration has capability for scoring/ ranking. The authority must recommend common rules for scoring of all TSPs in case of the present signature filtrations. The source of UCC may be identified based on the analysis of content of A2P/ P2P SMSs. Scoring system may be based on historical patterns, time of communication, mode of communication or depend on season especially in case of promotional messages.

ii. Regarding collaboration among access providers, some stakeholders suggested that it may be unwise to share the specifics of a signature solution with all entities, as this would help in creating UCCs that can bypass the signature solution implementations. However, if some access providers decide to work together, then they could selectively share information to help each other via a common secure platform that allows them to exchange information.

Intact Code

**5.3 Analysis of inputs and conclusions**

Following paras deliberates on the issues which are related to complaint handling. Issues and responses to the questions raised in the consultation paper are also summarized. Key points from the current regulatory approach and approaches taken in other jurisdictions to deal with the issues were also considered while analyzing inputs and concluding the issues. Analysis of inputs and conclusions of the Authority are as follows:

5.3.1 **Customer Complaint Registration Facility (CCRF):** Similar to the provisions in the current regulations, access provider should establish CCRF for its customers to make complaint(s). However, facility may be made more efficient and effective by automating most of the complaint handling processes. Considering computational resources and networking technologies which are available now-a-days, it is possible to reduce the time required to register and acknowledge the complaint. System can quickly check whether requisite information is available or more information is to be sought from the complainant. Mobile App may be very helpful for the customer to intuitively and intelligently select the probable telephone numbers which may be UCC. Mobile App also helps the customer to retrieve requisite information from the device to make complaint in a convenient manner. It avoids or eliminates chances of rejection of complaint on grounds of non-availability of requisite details. App can also pre-validate data and submit information to other systems in a structured form. This helps to automate the process and take quick actions. Web portal may also help in pre-validating data and submitting information in structured form. But in case of making complaints via web portal or using another phone number other than the phone number on which UCC was received, authentication may be required via OTP. And if customer is not using the mobile app or web portal, it is required to guide him or her about the procedure for making complaint. This may be done by providing information via SMS, referring to links to get more information or suggesting available alternative modes to make complaints. In view of this, **the Authority decided that complaint may be acknowledged by the access provider within fifteen minutes by sending unique reference number to the complainant. Processes**

**of CCRF may be automated and improved to make them more interactive in handling the registration of a complaint. Further specific details to handle registration of complaints may be included in the Codes of practice.**

5.3.2 **Technology driven solutions to handle complaints**: As discussed earlier in the para 3.3 and 4.3, Distributed Ledger Technologies (DLT) with complementing technology and platforms can record complaints in an immutable and non repudiable manner and can provide sharing of complaint related data, history of complainant, and history of person or entity against whom complaint is made easily accessible. Actions performed by participants in the UCC eco system while dealing with complaint resolution may also be made transparent and auditable. To deal effectively, DLT system could be designed to have the capability to swiftly and automatically throttle the usage of or suspend or remove the defaulting entity from the UCC eco system using smart contracts. As discussed earlier in Para 3.3, systems would be designed to make non-compliance from registered entities very difficult. By design the only instances of lapses would be in cases multiple participants deliberately introduce vulnerabilities in the system or due to mistakes in the configuration of the system. Proactive mechanisms to detect such occurrences and quickly isolate defaulting entity from the system would reduce chances of violations of regulations through UCC eco system of registered entities. In view of above, the **Authority decides that Access Provider should establish DLT based system(s), functions and processes to resolve complaints made by the customers and to take remedial action against sender(s).** Access Provider should establish Distributed Ledger(s) for Complaints (DL-Complaints) with requisite functions, processes and interfaces: -

i. to record complaints and reports regarding violation of Regulations made by the customer in the Distributed Ledger for Complaints (DL-Complaints) in an immutable and non repudiable manner;

ii. to record relevant details about the complaint or report regarding violation of Regulations.

iii. to record three years history of a complainant with details of all complaint(s) made by him, with date(s) and time(s), and status of resolution of complaints;

iv. to record three years history of sender(s) against which complaint is made or reported with details of all complaint(s), with date(s) and time(s), and status of resolution of complaints;

v. to interact and exchange information with other relevant entities in a safe and secure manner;

vi. to support any other functionalities as required to carry out functions provided for in these regulations;

vii. To provide *facilities for its customers to register complaints against Sender(s) of Commercial Communication and maintain complete and accurate records of status of resolution of complaints;*

viii. To examine and investigate complaints, take actions against defaulters and take remedial measures to ensure compliance with the regulations;

ix. To comply with any other directions, guidelines and instructions issued by the Authority *in this regard.*

5.3.3 For controlling UCC from unregistered telemarketers, all customers using telecom networks may be advised not to indulge in UTM activities, otherwise they may be put under Usage Cap or their telecom resources disconnected. Similarly, there is need to have provisions that principal entities (or business entities) do not indulge in UTM activity, directly or indirectly. Further, they may be made aware of these provisions by the access providers. System and processes are required that encourage entities to get

InfiaCom

registered and on-boarded to UCC eco system before making commercial communications. Measures specified in Para 3 and Para 4 are already part of such UCC eco system to better match the interests of sender and recipients, to protect the interests of business entities, and to permit the options for reaching out customers when there are legitimate and justified reasons.

5.3.4 **Entertaining complaints from customers not registered on DL-Preferences**: The present system does not have provision of lodging complaint by the customer who have not registered any preference(s). However, there are certain instances of violation of provisions of regulation like UCC from UTM, UCC beyond permissible hours etc., where unregistered subscriber may also like to register complaints. Such complaints may be treated differently compared to normal complaints by a customer registered on DL-Preferences. These may be referred as "reports" instead of "complaints". Complaints received after the specified time period from a customer registered on DL-Preferences or those with insufficient evidence may also be recorded as reports. Taking such complaints into account would help identify UTMs or RTMs who indulge in activities are not permitted under the regulations. When suspected UTM is sending UCC in bulk then only complaints which may be few in numbers may be relied upon. It would require defining meaning of bulk. Similar approach has been adopted in other jurisdictions such as in Singapore where in bulk is defined in the Spam Control Act (SCA) 2007, for details refer link https://sso.agc.gov.sg/Act/SCA2007. In view of this, **the Authority also decides to define bulk based on number of messages or voice calls made during 24 hours, seven days and thirty days**. **The Authority also decides that Access Provider should entertain reports from such customers for detection of bulk UCC sender and non-compliance of regulation. Access Provider may be required to consider all the complaints made within relevant time period of commercial communication. Even if the complaint is received after the specified time period, TSP should not reject it, but consider it as report for use in UCC detection.**

5.3.5 **System to Detect UCC**: To deal with UCC from UTM, signature solutions needs to be enhanced which shall be referred to as the UCC_Detect System. While determining whether a person or entity is suspected sender of UCC, this system may include additional sources of inputs such as sending information (SI) from reports, inputs collected from Honeypots, information shared by Signature Solutions of other access providers, information available from network elements e.g. HLR, miss call alerts etc. Such system would be able to identify suspected UTMs with greater accuracy when it is equipped with more information about suspected UCC senders. Technology based solutions can be designed to carry out all these checks and retrieve desired information in a short time. This system may also use Artificial Intelligence (AI) and Machine Learning (ML) techniques to constantly evolve to deal with new signatures, new patterns and new techniques used by UTM for sending UCC and while remaining undetected. Currently, criteria, rules, policies etc. for detecting UCC from UTMs are in public domain and spammers adapts their patterns to escape detection. Since taking action is permissible only after a complaint is received from at least one customer the criteria, rules and policies for detection should be treated as intelligence secrets and kept confidential. This system may also be helpful

i. ***to detect suspected senders after analysing multiple factors:*** *The determination of a UCC sender's guilt cannot be made on the basis of one single complaint. When a customer makes a complaint against a sender of UCC, there should be a system to immediately check whether any other recipients have filed similar complaints about the same sender. For this purpose, supporting information may be provided by this system after analysing multiple factors other than complaints and signatures, such as profile of the customer may be helpful in avoiding false positives. Reputation-based analysis may take into account various factors like age of subscription, authentication at the time of subscription, address verification method etc.*

ii. ***to detect unauthorized senders of content****: UCC_Detect System may also support pattern*

InfiaCore

*matching to be applied on A2P (Application to Person) traffic coming from RTMs. It may be useful to detect messages sent by unauthorized entities e.g. investment tips sent by entities who are not registered with SEBI or header being used for sending traffic for which it was not intended at the time of assignment. This may require enhancement of current signature solution to also have list of headers along with the purpose for which they are assigned.*

iii. ***to exchange information among similar systems of other access providers****: Access providers should develop a scoring system for UCC to detect UTMs operating using telecom resources from different access providers. While developing such scoring system access providers should consider outcome of 3GPP Technical Study Report TR 33.937 "Study of Mechanisms for Protection against Unsolicited Communication for IP Multi-Media Sub-system (IMS) (PUCI)" which describes concept of Unsolicited Communication (UC) score and also details out option to exchange information about UC score among different entities using IP Multi-Media Sub-system (IMS).*

In view of this, **the Authority decides that Access Provider should establish UCC_Detect System with requisite functionalities to detect, identify and act against sender(s) of Commercial Communication who are not registered with them and to detect unauthorized senders of content, e.g. related to financial investment tips, advisories. Further implementation details about UCC_Detect_System need to be included in Code of Practice (CoP) for such system.**

5.3.6 **TAP and OAP to act in parallel for timely action to control UCC**: Reduction in time for complaint registration and its resolution may be achieved by adopting technology-based solutions. This would require automation of processes and development and deployment of APIs. Once complaint is registered, there are multiple reasons for delays in resolution. One reasons may be that TAP, and OAP deal with the UCC complaints in a sequential manner. Sometime gains can be made by parallelizing some of the processes. It is recommended that TAP should immediately record the complaint and forward it to the OAP for resolution. In the meantime, TAP may check CDRs of the complainant and/or the person or entity complained against to verify the occurrence. The outcome of this check may be recorded on Complaint Handling System which is also accessible to OAP. In view of above, **the Authority decides that TAP should record the complaint and notify, in real time, the details of the complaint to the concerned OAP. TAP should verify within one business day, whether the alleged communication actually occurred between the complainant and the reported telephone number or header and update the findings on distributed ledger. TAP should also verify that date of receipt of complaint is within three days of receiving commercial communication and in case complaint is reported by the customer after three days, communicate to the customer about the closure of his complaint in accordance with the Code of Practice for Complaint Handling and change status of complaint to "report" instead of complaint.** Business are usually closed on Saturdays, Sundays and Gazette holidays declared by Central Government and time required to act against UCC complaints may need to consider this. In view of this **definition of "Business Day" was changed to any day other than a Saturday, Sunday or Gazette holidays declared by Centeral Government.**

5.3.7 **Issues with a single stage investigation process:** The severity of punishments which are prescribed for offenders, is another reason investigation takes time. Currently, if a complaint against a UTM is found to be valid it leads to disconnection of all telecom resources belonging to that entity. Moreover, such person or entity is also blacklisted and cannot take resources from any of the access provider for a period of two years. In case of RTMs for the first five violations, the action is deduction from security deposits, and deductions increase for each violation. After six violations, the RTM is blacklisted. This puts the access provider on cautious path as hurriedly concluding the investigation may lead to victimization. This creates situation in which taking action against UCC in aggressive manner leads to increase in wrongful actions and comprehensively investigating the cases leads to complaint resolution

Indiacode

taking a long time. Sometimes the fact that resolution takes a long time is exploited by spammers or entities deliberately defaulting to send UCC.

5.3.8 **Introduce multi-stage investigation process to control UCC**: The Authority is of the view that the aforementioned issue could be solved by making investigations multi-staged. The first stage, should be of preliminary examination of the complaints, if it is found that the person or entity against whom complaint is made is likely to be a spammer or sender of UCC in bulk then their facility to communicate should be temporarily restricted. For example, if a number is suspected of sending UCC in violation of regulations, their outgoing usage could be capped without restricting incoming calls, SMS and Internet. This cap would be in place until the investigation is concluded. With this change in approach, action may be taken quickly to address the UCC problem while sufficient time is available to comprehensively investigate complaints. Such control measures are to be applied within two business days of receiving the requisite number of complaints.

5.3.9 It is observed that UTMs usually have pre-paid customers but there may be instances of UCC from UTMs having post-paid customers. It is more likely to happen in cases of business entities or corporate connections. In case of post-paid customers, unlike pre-paid customers, usage is not checked by the system at the moment of initiating service request and it may be required to explore ways and means to implement Usage Cap for post-paid customers. For example, post-paid customers against whom Usage Cap is to be applied may be temporarily configured as Intelligent Network Subscriber to apply Usage Cap. Other options for post-paid customers to effectively implement Usage Cap would be prescribed while formulating codes of practice to be formulated by the access providers.

IndiaCore

5.3.10 **Preliminary Examination of Complaints by OAP**: To deal with complaints related to RTM, both the TAP and OAP have to investigate and resolve the complaint in parallel. Action against the RTMs must be part of Code of Practice for Complaint handling. As discussed earlier in Para 3.3, UCC eco system is to be controlled and managed by the access provider and specific actions to be taken against RTMs would be part of CoPs. Access provider's performance in terms of keeping a check on RTMs would be measured on the basis of aggregated complaints received by OAP against RTMs. OAP should carry preliminary examination of the complaints in two days so that appropriate action may be taken against suspected sender of UCC. In view of above, For OAP, **the Authority decides that in case the complaint is related to RTM, OAP should examine, within one business day from the date of receipt of complaint, whether all regulatory pre-checks were carried out in the reported case before delivering UCC, and in case, answer is yes then OAP should communicate to TAP to inform complainant about the closure of complaint as provided for in the Code(s) of Practice. In case, answer is no, then OAP should, within two business days from the date of receipt of complaint, take actions against the defaulting entity and communicate to TAP to inform the complainant about the action taken against his complaint as provided for in Code(s) of Practice.**

5.3.11 **Structured way to deal with complaints against suspected UTMs**: The Distributed Ledger for Complaints (DL-Complaints) having histories of complainant and against whom complaints are being made used in conjunction with UCC_Detect_System would make it possible to precisely identify UTMs. This approach would minimize victimization, while effectively detecting UTMs and prevent them from sending UCC. In view of above, **the Authority decides that in case of complaint against a UTM also the OAP should examine CDRs in parallel to TAP, within one business day from the date of receipt of complaint, to check the occurrence of communication that is under investigation. In case, answer is no, then OAP should communicate to the TAP to inform the complainant about the closure of complaint in a manner prescribed in the CoP. In case answer is yes, then OAP should further examine, within two business days, whether there are similar complaints or reports against the same sender**.

i. *Action should be expedited to control UCC, if multiple complaints are received against same*

*sender, Usage Cap should be applied immediately, which may be restored after due investigation if there is no guilt. Suffiicient time should be given for concluding the investigation as opportunity must be given to the sender who is kept under Usage Cap to defend themselves.* ***The Authority decides that if there are complaints against the sender from ten or more recipients over a period of seven days preceding the date of receiving complaint, the OAP should put the sender under Usage Cap and at the same time should initiate investigation. Such restrictions should be in place till investigation is complete or for thirty days from the date of effect of restrictions, whichever is earlier.***

ii. *If complaints are not received from multiple recipients then before taking action, more checks should be done to find out whether sender has sent only few messages or made only few calls and can not reasonably be considred as UTM. In vieew of this* ***the Authority decides that where number of complaints are from less than ten recipients, the OAP should, check from the previous thirty days data of CoP_UCC_Detect System whether suspected sender is involved in sending Commercial Communication in bulk or not*** *(Definition of bulk may be by counting communications over a period of 24 hours, over a week and over a month).*

a. **in case, answer is yes, the OAP should put sender under Usage Cap and at the same time initiate investigation.** Such restrictions should be valid till investigation or thirty days from the date of effect of restrictions, whichever is earlier.

b. **in case, answer is no, OAP should warn such sender through appropriate means as provided for in CoPs and remove the usage cap**.

iii. *Sender should be given opportunity to represent his case before finally concluding the investigation. If sender was found indulging in UCC in violation of regulations, he should be given warning for the first offence and the Usage Cap removed. If the violation is repeated a second time, Usage Cap should be applied for longer period and in case of third time, all resources should be disconnected except one which may be provided with Usage Cap to use minimum functional requirements for daily use. In view of this* ***the Authority decides that OAP should issue notice, within three business days, to give opportunity to suspected sender(s) to represent his case and conclude investigation within thirty business days from the date of receipt of complaint and if sender is found to be indulging in sending UCC then OAP should take action against such sender as under:*** *-*

a. **for first instance of violation, due warning shall be given.** First instance of the violation should include all the complaints against the sender within two business days after the date of receipt of the first complaint, against which the sender is to be warned.

b. **for second instance of violation, Usage Cap should continue for a period of six months.** Second instance of the violation should include all the complaints against the sender after the issuance of first warning within two business days after the date of receipt of the complaint against which second warning is being given to the sender.

c. **for third and subsequent instances of violations, all telecom resources of the sender shall be disconnected for a period up to two years**.

5.3.12 **Review of structure of financial disincentive for access providers**: At present, access providers are subject to financial disincentive if UCC complaints are found to have originated from their network. Financial disincentive for UCC complaint are being imposed on weekly basis and the provision of financial disincentive is applied even when UCC complaints are handled within given time frame and expected action is taken against UTM or RTM. At the time of amendment of the regulation for this provision, it was felt that Access Providers are responsible for carrying out due checks and verification of the customers and if bulk connections are being taken by customers and being misused then Access Providers are not discharging their due responsibilities. TSPs have represented, from time to time, against applying financial disincentives on counts of UCC complaints including even those UCC

Intellectual

complaints on which they have taken timely action.

i. *In new regulatory framework where co-regulation approach is being adopted and COPs are to be formulated by the access providers, primary responsibility to control UCC is of access provider. OAPs failing to curb the UCC sent through its network(s) should be liable to pay by way of Financial Disincentives. The FDs should be telescopic; i.e. nominal if the number of incidences reported are below a threshold, but substantially higher if the number of cases beyond a certain threshold. In new regulatory framework, technology driven systems are to be put in place and access providers are given flexibility to act fast against the defaulter entities. It may also be noted that access providers are also given freedom to prescribe charges/ fees and access providers can also impose financial disincentives on defaulting entities for faults attributable to them. In such situation graded financial disincentives should be applied and it should increase substantially in case number of complaint rises against RTMs. In view of this* ***the Authority decides that FD for access provider, in case of complaints related RTMs should be based on the Count of UCC for RTMs for one calendar month in each License Service Area. It should be increased to Rs. one thousand per count if it is more than zero but not exceeding hundred. This should be increased to Rs. one lakh plus Rs. five thousand per count exceeding hundred when count is between one hundred and one thousand. This should be further increased to Rs. forty-six lakhs plus Rs. ten thousand per count exceeding one thousand when total count is more than one thousand.***

ii. *Access providers are supposed to take action against UTMs suspected of sending UCC and also carry out due investigation and take appropriate action against the UTMs. Normally it is expected that access providers would be following processes and not to be held responsible for UCC from UTMs. Access provider would also be required to inform their subscribers to not send Commercial Communication or cause sending Commercial communication or authorize the sending of the Commercial Communication using the telecom resources failing which the telecom resources used or assigned to him may be put under Usage Cap or disconnected.*

iii. *Access providers would have to establish UCC_Detect system to control UCC from UTMs. If access providers do not act against the detected UTMs in a timely manner, then they may be held accountable for not controlling UCC. If it comes to notice or is found during audit of the system that the access provider has not taken action against UTMs as specified in the regulations or CoPs then access provider may be liable to pay by way of financial disincentives. The FD in case of UTM may be dependent on every such instance. In view of this* ***the Authority decides that Financial Disincentive of one lakh per instance of access provider failing to impose timely restrictions on outgoing usage of unregistered sender(s) be imposed on the access provider.***

iv. *In view of UCC eco system based on DLT is created by the access provider(s) and measures taken to control the outgoing usage of telecom resources of suspected sender of UCC whenever it comes into notice, current provisions of Financial Disincentives for access providers may need to be revised. Access providers are supposed to apply Usage Cap within timelines prescribed in the regulations. If it comes to notice of the Authority that access provider is not taking such measures in timely manner and same is established through special audits and no satisfactory justifications for any delay in applying such measures, then access providers may be liable to pay by way of financial disincentives.*

5.3.13 As discussed earlier in Para 3.3, further specific details should be part of Codes of Practice for Complaint Handling (CoP-Complaints) and Code of Practice for UCC_Detect_System which should be formulated by the access providers. In view of this **the Authority decides that access providers shall also formulate codes of practice for complaints (CoP-Complaints) and codes of practice for UCC Detect system (CoP-UCC_Detect).**

5.3.14 Access providers may also be liable to pay by way of financial disincentives in case they do not establish eco system in accordance with the codes of practice. Such disincentives may be applicable till such system comes into existence and made live to deal with relevant aspects. However, after implementing such systems in accordance with the CoP, if non-compliance occurs due to some flaw in implementation or inappropriate configurations of the system then financial disincentives may be applicable in accordance to the provisions under count of UCC complaints and not against non-implementation of CoP. For example, if access provider has not implemented systems and process as defined in the codes of practice and UCC complaints are on rise due to non-implementation of CoP then financial disincentives may be applied for non-compliance of CoP. If access provider has implemented the system and subsequently UCC complaints are rising because of some issues related to system, then financial disincentives for non-implementation of CoP would not be applicable. Financial disincentives as applicable for UCC counts may be levied. However, if there is major non-compliance of CoP on part of system or there are multiple minor non-compliances in the system which amount to as complete failure of the system then financial disincentives for non-compliance of CoP may be applicable.

5.3.15 **Developing and enhancing mobile App for all device OS**:

i. *In present day and age where technological advancements have been made, smart mobile phone devices aren't just a means to make calls but have acquired intelligence and are integral part of the telecommunication service/network. In order to maximize such intelligence, the application Do Not Disturb App ("DnD App") developed by TRAI or such similar applications developed by third parties with due approval of TRAI, facilitate in an easy, efficient and effective manner reporting and resolution of UCC and advance telecommunication consumer interest.*

ii. *Undoubtedly, such applications are one of the most effective means for subscribers for registration/ deregistration/ change of preferences, checking the status and handling complaints pertaining to UCC.*

iii. *Such Apps seek customers' permission to access the SMS and call logs on the mobile device. This requirement has been viewed by some stakeholders to be a violation of customers' privacy.*

iv. *This is an incorrect perception because the DND App (or a functionally equivalent App) requires access to the logs only to present to the customer what is his or her own data, also accessible by the customer in other ways. Further, the customer initiates every action based on the information presented, while the App merely provides assistance in completing the action as per regulation. At no time does the App require access to these logs for other purposes, nor does it transmit the information to anyone other than the entity with whom the customer himself or herself wishes to share the information.*

v. *An issue raised by some stakeholders is that TRAI doesn't have the power to regulate devices. However, it is TRAI's statutory duty to safeguard consumer interest as indicated in the TRAI Act: "... to protect the interests of service providers and consumers of the telecom sector, to promote and ensure orderly growth of the telecom sector, and for matters connected therewith or incidental thereto." With the intelligence residing in the nodes and end devices, the network cannot operate totally independently of the user equipment. Such elements of the equipment that affect the performance of the network or the experience of some or all its users (which is "connected therewith or incidental thereto") may be regulated as necessary in the discharge of TRAI's statutory obligations.*

vi. *"Regulate" means to control or to adjust by a rule or to subject to governing principles. It is a word of broad impact having wide meaning comprehending all facets not only specifically enumerated in the Act, but also embraces within its fold the powers incidental to the regulation*

Draft Code

*envisaged in good faith and its meaning has to be ascertained in the context in which it is being used and the purpose of the statute. The regulatory power possessed by the TRAI shall also include the power to regulate all the things incidental to the telecommunication sector. If the matters incidental to the telecommunication sector is read in a restrictive manner, then it will not be fair whereby the provisions made for the benefit of the consumers become wholly illusory. The expression regulatory is to be given expanded meaning and has been construed liberally so as to achieve the object stated in law.*

vii. *Further, where a statute gives a power, such power implies that all legitimate steps may be taken to exercise that power even though these steps may not be clearly spelt in the statute. Where the rule making authority gives power to certain authority to do anything of public character, such authority should get the power to take intermediate steps in order to give effect to the exercise of the power in its final step, otherwise the ultimate power would become illusory, ridiculous and inoperative which could not be the intention of the rule making authority.*

viii. *The purpose of enacting the TRAI Act, was as stated hereinbefore, generally, to regulate the telecom sector, and in particular to safeguard the interests of the consumers of telecom services. Thus, the entire Act, especially mandatory functions of the TRAI, will be read in this perspective. Therefore, an intelligent telecommunications network element such as a smart mobile handset cannot and should not be allowed to frustrate the basic objective of the Act.*

ix. *As far as derecognition of devices is concerned, TRAI based on the grievances from the customers would make a decision regarding whether the device needs to be derecognized by the service providers or not based on whether any device is contravening the Regulation or not. It is not expecting from the service providers to take responsibility of the device manufacturers in supporting the DnD App or such similar Apps but would only direct the service providers to derecognize such smart mobile phone devices on their network which do not support the functionality of such App on their device platform.*

x. *Smartphone is defined in GSMA official document TS.06 regarding IMEI Allocation and Approval Process, for details refer https://www.gsma.com/newsroom/wp-content/uploads/TS.06-v13.0.pdf*

In view of this, **the Authority decides that Access Provider should ensure, within six months' time, that all smart phone devices registered on its network support the permissions required for the functioning of such Apps. If such devices do not permit functioning of such Apps then Access Providers shall, on the order or direction of the Authority, derecognize such devices from their telecom networks. However, before issuing order or direction of derecognition of devices, the concerned parties may be given a reasonable opportunity.**

5.3.16 **Scrubbing as a Service**: As discussed in Para 3.3.4, Para 3.3.5, Para 4.3.1 and Para 4.3.4, Scrubbing may be offered as a Service using DLT networks and Scrubbing Function may be delegated to any other entity, if the processes can be run in an environment which is safe and secure during information exchange and execution. Using DLT networks, safety and security may be provided in a multi participant environment with peer to peer and distributed environment approach.

5.3.17 **Auto Dialler Calls, Silent Calls and Robo Calls**: Issues and concerns related to Auto dialler calls, silent calls and robo calls have already been deliberated in Para 4.3.15 and the recommendations of the authority have also been mentioned there in Para 4.3.16. To reiterate, **the Authority decides that the sender be allowed to use auto diallers only when they notify the access provider in advance and take necessary steps to keep silent calls and abandoned calls within limits as prescribed, from time to time.** However, for the impact of Robo calls, is still not clear and requires further examination. Authority is of

InfiCode

view that such calls should be closely watched, and appropriate action may be initiated against when more information is available.

5.3.18 **Record keeping and reporting:** Access Provider should maintain records of complaints, from its customers and those received from TAP(s), against registered sender(s) and unregistered sender(s) on daily basis for each service area and submit performance monitoring report to the Authority as and when required in a format as prescribed. For periodic reporting of the performances of UCC regulation, Code of Practice for Reports (CoP-Reports) may also be formulated. Other requirements for CoP may be same. In view of this **the Authority decides that access providers shall formulate codes of practice for submitting reports (CoP-Reports) and this should include summary of outcome of complaints handling at different stages and for different scenarios. The Authority may also conduct audit either by its own officers or employees or through agency appointed by it, verify and assess the process followed by the access provider for registration and resolution of complaints, examination and investigation of the complaints and reporting to the Authority.**

5.3.19 **Examination of telecom resources put under outgoing Usage Cap or having been disconnected:** Similar to provisions under current regulations, the Authority may ask access provider to restore the connection or remove the Usage Cap after conducting an investigation. **The Authority may direct the Access Provider to remove restrictions on usage or restore all telephone number(s), If the Authority finds that conclusion of investigation against sender of UCC lacks adequate evidence against the sender. The Authority may also ask Access Provider to restore capping on usage or restore telecom resources from disconnection if the sender whose resources have been put under Usage Cap or disconnected satisfies the Authority that he has taken reasonable steps to prevent recurrence of such contravention however some charges for restoration or removal of usage capping may be applied.**

5.3.20 **Power to appoint inquiry committee:** It is observed that many times principal or business entities are taking services of other entities dealing in telemarketing activities. Such entities may be registered telemarketers or unregistered telemarketers. It may also happen that principal entities have tied up with registered telemarketers, but RTMs may be in nexus with UTMs to send UCC. From the UCC complaints or reports, it may come to notice that primary motive of sending UCC is of principal entity and they have either not taken appropriate measures to comply with the regulations or deliberately indulged in sending UCC. In such cases, it may be required to investigate the matter and take appropriate actions against defaulter principal entity found to be indulged in such activities. If the Authority believe that any sender of commercial communications on behalf of business or legal entities has contravened the provisions of these regulations, it may constitute an inquiry committee, to inquire into the contravention of the regulations and to report thereon to the Authority. In case, it is found that particular business or legal entity is engaged in sending commercial communications in contravention to the provisions of these regulations, the Authority may order or direct access provider(s) to disconnect all telecom resources or put all telecom resources of such business or legal entity under Usage Cap of such telecom resources.

## 6 Need of Technology driven framework for UCC

**6.1** Efficient and effective way: Authority has always encouraged adoption of technology driven and data driven approach for efficient and effective regulatory compliances. New technologies and innovative processes may have the potential to achieve speed where regulatory pre-checks are required to be carried out for enormous transactions.

**6.2** **Regulatory Checks in distributed environment:** Technology driven solutions are required to control menace of Unsolicited Commercial Communication (UCC). In case of UCC, the technology needs to work in distributed fashion and ensures that necessary regulatory checks are performed. Technologies and

Under Code

solutions based on it should create records for every action taken by the different entities to check regulatory compliance before and after delivery of commercial communications in an immutable and non-repudiable manner. Regulatory checks in case of commercial communications are based upon present status of preferences and consent of the customer. These preferences and scope of consent are evolving and may become more and more comprehensive and granular in the future to match interest area of the customer. This evolution will be on both, the customer's side and as well as business entity's side. The selected technology solutions should provide a framework which adapts itself to meet such requirements and provide capability to carry out regulatory pre-checks in an immutable and non repudiable manner.

**6.3** **TSPs to ensure other entities perform requisite checks**: Responsibility of honoring choices exercised by the customer while delivering commercial communications may require checks to be made by number of entities in content delivery chain. However, primary responsibility of protecting customers from UCC is of Telecom Service Providers (TSPs) which is a licensee and regulated directly. Other entities in commercial communication system are currently being regulated indirectly via standard agreements in which they have entered into while taking telecom resources from TSPs. Technology solutions may provide better grip in the hands of TSPs who may be primarily responsible to control UCC and honour choices exercised by the customers.

**6.4** **Standard Agreements prescribed via regulations to ensure checks by other entities**: To ensure regulatory compliance for UCC, TSPs should be required to keep preferences of its customers about the types of commercial communications in which they are interested in and other types of commercial communications in which they are not interested. Customers expect that their service providers will take suitable measures for blocking unsolicited commercial communications. However, message sending entities or voice calling entities, who wishes to reach out to customers are huge in numbers and spread across the country and TSPs may not be in position to control them centrally. The task of checking compliance will consist of matching list of recipients with the list of preferences and consents with the category of content of communication and identity of content providers. This may be practically difficult to be carried out by TSPs alone. TSPs may need to delegate some of the functions to various other entities to meet the regulatory requirements. The unbundling and delegation of specific functions for regulatory compliance may lead to the creation of a complex web of a large number of entities interacting in real time. These agreements between these entities may need to be changed often to ensure regulatory compliance in changing and evolving requirements. The selected technological solutions must be able to provide capabilities to TSPs to supervise this large, complex network of entities and take necessary actions remotely, but in real time. In this way, TSPs may quickly respond to the situations and evolve to deal with UCC constantly changing its nature and to ensure UCC regulatory compliances in changing environment.

**6.5** **More trusted relationship between Terminating Access Provider and Originating Access Provider**: Technology solutions may help to build more trust between TAP and OAP for the entities which are registered to carryout regulatory compliances and actions performed by them. It may be noted that practically there is a web of entities between content providers or principal entities and TSPs. Even TSP to which subscriber belongs to (known as TAP) may not be having direct connectivity with the entity e.g. telemarketing traffic directly from the telemarketer and it might be coming via other TSPs known as Originating Access Providers (OAPs). Due to this situation, technologically regulatory compliance for UCC is distributed among various entities and technology solution may build more trust for the TAP for actions performed by the entity which is not connected directly with it.

**6.6** **Building more confidence in the UCC ecosystem for the Principal entities**: Principal Entities (PE) are primarily interested in reaching out to the customers for the purpose of commercial communications,

IndiaCode

telemarketers may be just be facilitating them with their arrangements with TSPs to deliver content and carrying out necessary regulatory checks. Practically, principal entities and content providers so far may not be directly part of regulatory regime for UCC as they are not registered and may not have entered into any of legal agreements specifically for purpose of UCC regulatory requirements. They ask their channel partners or Direct Sales Agents (DSAs) to become Telemarketers or have tie up with telemarketers to deliver commercial communication content and measures to comply with UCC regulations is with telemarketers. As a result, although obligations of regulatory compliance may be with TSPs and key interests in commercial communications may be of principal entities or content providers but so far, practically strength of whole regulatory compliance framework rests upon technological capabilities of systems available with the telemarketers or in their seriousness to carry out regulatory checks rigorously. Telemarketers in the front layer of web of entities towards TSP (i.e. telemarketers who have taken telecom resources from TSPs) enters into standard agreement while there is no standard agreement between rest of entities in the subsequent layers of entities which are towards content providers' side. Even if standard agreement is mandated for all such entities in the chain, practically it may remain ineffective till technology driven monitoring and enforcement mechanism is available with TSPs to overall ensure regulatory compliance through these entities.

**6.7** **Concerns of PEs**: Another issue to principal entities or content providers is to have protection to their client database and there is a need of technology solution which allows UCC regulatory checks to be performed by various entities in such a manner that client database remains protected.

**6.8** **Using sensitive information in secure manner:** Technical possibility to restrict Commercial Communication to Customer in certain scenario which needs customer's information e.g. restriction while roaming may require location information available to external entities for applying requisite checks. Technology solution may need to be explored which enables such additional checks at TSP level while rest of the checks have been carried out earlier.

**6.9** **Objectives to be met by technological solution**: New technology may play increasingly pivotal role in UCC regulatory space and augment capabilities of almost all entities of Commercial Communication ecosystem, offering consumers and markets easier access to, and better control and management to TSPs for commercial communication services. Technology solution may be required to support to meet three key objectives with regard to commercial communications:

- Protect consumers – to secure an appropriate **degree of protection** for consumers
- Protect interests of telecom service providers – to **enable better control and management** of TSPs over entities delivering commercial communications through them to avoid levying financial disincentives in case of non-compliances by ensuring regulatory compliances through technology driven solutions
- Promote competition – to continue **multiplicity of players to participate** in the commercial communication ecosystem.

7 Distributed Ledger Technology (DLT) can provide requisite capabilities:

**7.1** Authority deliberated on the issues of regulatory requirements and operating models, that would be suitable to spearhead efforts to solve real business problems in dealing with UCC. Given the scale of the participating entities within the commercial communication market, the Authority is of view that DLT is the best match for meeting regulatory and operational objectives. Following section provides a thorough discussion on how DLT can potentially address a wide range of business, regulatory, legal, and technical issues related to Commercial Communications and help in controlling UCC.

**7.2** **DLT solutions are smart**: Ledgers have been used to record many things and these were traditionally

mostly on paper. Gradually we have seen record-keeping system evolve, and these ledgers have moved from paper to bytes. State of the art systems are now moving towards digital distributed ledgers with properties and capabilities that go far beyond traditional paper-based ledgers. DLT solutions have the potential to transform ledgers to enable recording of an enormous number and range of transactions in a secure manner. They can also integrate business rules, smart contracts, digital signatures and an array of other tools with the basic functionality of a ledger which is to record transactions (or more generally changes of state).

**7.3** **DLT is Resistant to unauthorized changes**: As a result of the methods by which information is secured and updated in a DLT-based record, participants can be confident that all copies of the ledger will match each other at any given point of time. Any changes to the ledger are visible to all participants, and changes are only incorporated after a consensus is reached among participants regarding the change. Thus, the record is resistant to unauthorized change or malicious tampering, and participants in the network will immediately be able to spot any change to any part of the ledger.

**7.4** **DLT Replicates data with security and accuracy**: A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated **by one, some or all of the participants, according to rules agreed by the network.**

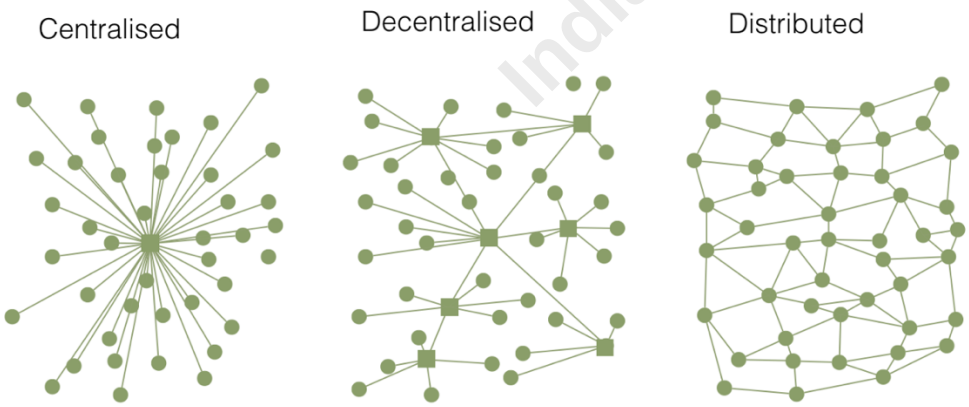



*Figure 14: Difference between Centralized, Decentralized and Distributed Architecture*

## 8 Important properties of DLT

**8.1** **Reconciliation Through Cryptography:** In DLT networks different actors (users) of the ledger come to a consensus about the state of the underlying data through consensus algorithms (e.g. Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance).

**8.2** **Replicated to Many Institutions:** In DLT networks, many parties can have a copy of some or all of the data, making it less likely to have a single point of failure. An additional benefit of this technology is that if one ledger is compromised, the remainder are not. Many parties can also confirm that those records have been added by performing the reconciliation calculations themselves.

**8.3** **Granular Access Control**: Distributed ledgers use 'keys' and signatures to control who can do what inside the shared ledger. These keys can be assigned specific capabilities and can be designed in a way that can only operate/ function under certain conditions.

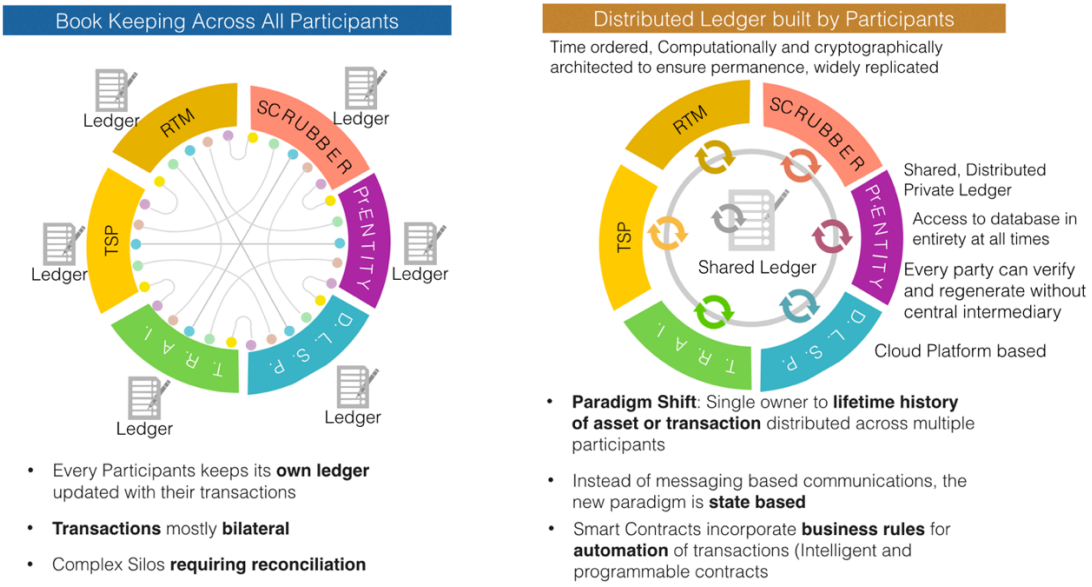



*Figure 15: Comparison of implementation of record keeping between traditional and DLT based systems*

**8.4** **Transparency and Privacy**: Because many parties have a copy of the ledger, and many parties can verify every record, a shared ledger has a high degree of transparency. This can enable a participant with the right access privileges (e.g.: regulator or an independent body) to ascertain with confidence whether the contents of a database have been edited or modified in any fraudulent way. Records are added with a cryptographic signature that is unique to each participant. This allows the entity examining the ledger to determine whether the right participant added the right record according to the right rules.

**8.5** **DLT has potential to offer solution**: Distributed ledger technology (DLT) seems to have the potential to support the needs of Telecom Service Providers, Telemarketers, Mobile Users for commercial communications with better control and management over UCC.

**8.6** **Automation, Flat architecture, Speed, sharing of data, shared cost:** DLT has the potential to provide various benefits for processes of registration of entities like telemarketers, content providers and identities like SMS headers, Calling line identities for voice calls. These benefits are likely to emerge in commercial communication space as multiple participants need to share data and processes safely, particularly for registration of entities and consent taking process where firms are still reliant on paper-based records. DLT's also have ability to remove certain unnecessary intermediaries which in turn will reduce the means for content providers to bypass regulatory compliances. The distributed nature of DLT based records, can increase the speed of making latest updated data available for scrubbing, complaint handling, reconciliation to multiple involved parties. It can also reduce cost and reducing costs makes it most promising option for adopting it as a regulatory technology for control and management of commercial communications.

**8.7** **Adaptability of DLT to meet evolving requirements**: In commercial communication space, nature of content of communication, preferences of customers are constantly evolving and may require regular update of business rules which are to be followed. DLT's can be designed to integrate intelligent and programmable contracts and business rules with bookkeeping functions. The functionality can be combined with the machine learning algorithms to give it the flexibility and agility which is necessary in a technology which is intended to be used to regulate the compliances for commercial communications ecosystem. Further, the creation of DLT systems as shared infrastructure will allow TSPs to ensure regulatory compliance of UCC norms while optimizing the capital and operational expenditures. DLT

therefore has many advantages in terms of efficiency and effectiveness.

**8.8** When combined, these properties can solve challenges of UCC regulatory checks and compliance that were previously very expensive or challenging. For the reasons discussed above, DLT seems to have exciting potential to support the needs of TSPs, Telemarketers, users for commercial communications with better control and management over UCC.

## 9 Types of DLT Networks

**9.1** **Multiple types of DLT networks**: In practice, there is a broad spectrum of distributed ledger models, with different degrees of centralization and different types of access control, to suit different business needs. These may be 'unpermissioned' ledgers that are open to everyone to contribute data to the ledger and cannot be owned; or 'permissioned' ledgers that may have one or many owners and only they can add records and verify the contents of the ledger.

**9.2** **Matrix of feature set for types of DLT networks**: In case of permissioned private ledgers, only permissioned entities may read the contents of the ledger and write to the ledger. The permissioned private ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors. This process makes data entry and verification faster and more efficient when compared to the consensus process of permission less ledgers. In addition, use of digital signatures by nodes on the chain also creates highly-verifiable data sets.

Intracode

**9.3** **Permissioned DLT Networks:** Permissioned (usually private) DLT Networks are often split into consortium DLT Networks, or fully private DLT Networks. There are benefits and drawbacks to permissioned, permission less, public, and private approaches, and combinations thereof. With permissioned private DLT networks there is an inherent trust as the users must be given consent by a governing body or entity to participate in that DLT network. This 'trust' reduces the amount of computational power required for that DLT network, as well as increases the speed of the DLT network. In case of permissioned DLT networks, participants are pre-approved, identities are known and only member of consortium can validate transactions. From the UCC regulatory framework perspective, a permission private consortium DLT network seems to be the most suitable regulatory technology (RegTech) for all stakeholders. For TSPs, application of DLT-powered RegTech solution for UCC regulation will lead to lower compliance cost. In addition to governance of DLT network(s) by entities operating it, observer nodes of this DLT network available with TRAI or any agency authorized by TRAI for supervision and audit purposes.

**9.4** In view of above**, the Authority decides that Access Providers should adopt Distributed Ledger Technology (DLT) with permissioned and private DLT networks for implementation of system, functions and processes as prescribed in Code(s) of Practice to ensure that all necessary regulatory pre-checks are carried out for sending Commercial Communication and to operate smart contracts among entities for effectively controlling the flow of Commercial Communication**.

**9.5 Suitable model of DLT Network for Spam control:**

9.5.1 Consortium of TSPs may be responsible to take decisions for changes required in the process of operation of DLT network(s) while they may outsource architecture of solution, installation, operation and maintenance of DLT networks to a separate entity, referred to as the DLT system operator. For selecting DLT system operator and type of DLT suitable for Permissioned Private Consortium DLT network, policy should be open and non-exclusive. However, there may be reasonable eligibility criteria to have functional and performance capabilities to achieve objectives of UCC regulatory compliances and maintain business continuity and coexistence of systems with requisite interoperability requirements.

9.5.2 Distributed ledgers have the added advantage of moving a lot of the complexity of managing security into the background, making systems easier and cheaper to use.

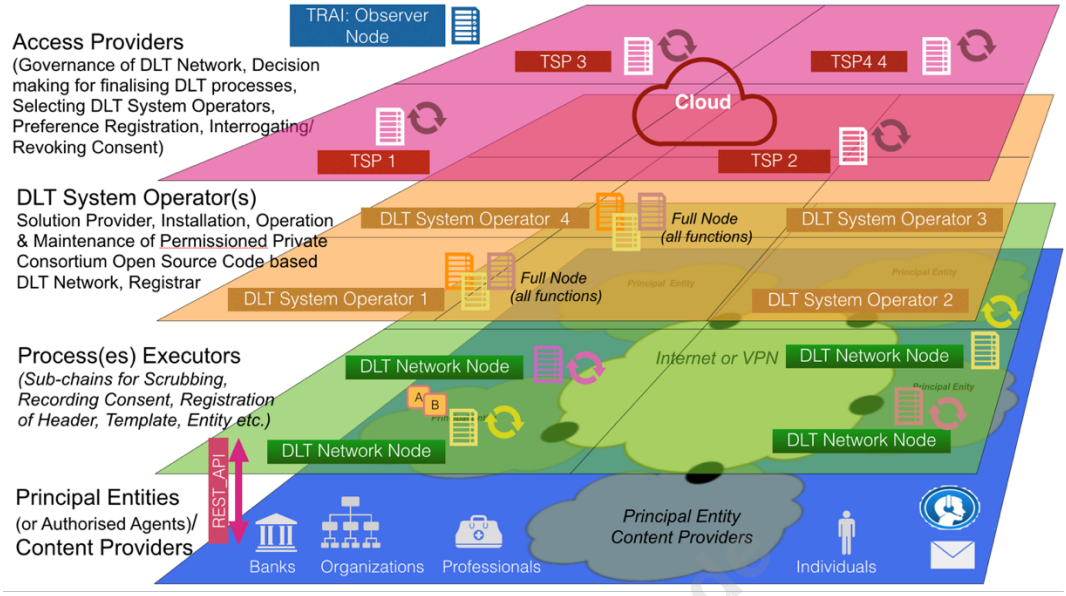



*Figure 16: : Illustration of architecture for implementing UCC eco system based up on DLT*

9.5.3 The adoption of DLT could take many forms and it is reasonable to assume that a number of DLT systems will need to interact and share data between one another and with non-DLT legacy systems. Therefore, at this stage, it may be difficult to specify any particular choice of DLT system. However, it would be appropriate to consider adopting DLT systems which offer open source-based implementation and have the capability to inter-operate with other similar open source based DLT systems and non-DLT legacy systems. Successful proofs of concept to meet the regulatory requirements of the UCC ecosystem and considerations such as interoperability with the incumbent systems and the ease and cost of adoption may be essential requirements to set up and participate in the new DLT system.

9.6 **Summary about DLT's potential:** DLT offers a revolutionary solution to fundamentally improve the regulation and delivery of commercial communications. As mentioned above, DLT allows all players in the ecosystem to share customer information and transaction histories securely over a distributed data infrastructure, with the consent of the user and without compromising on the customer's privacy or sensitive business information. The ecosystem's participants can be certain of the digitized records being authentic and are informed in a timely manner of the progress of the scrubbing and delivery of the commercial communication. Content providers and principal entities can therefore be sure about regulatory compliances and safety of their data along the delivery chain. Authority generally takes a 'technology neutral' approach but feels that DLT has distinctive features, which provide capabilities in hands of TSPs to control and manage commercial communications in more efficient and effective manner and meet their obligations to ensure UCC regulatory compliance.

9.6.1 It is encouraged to have single DLT networks which is shared among all access providers. In case, all access providers do not reach to a consensus to form single network, it is desirable to keep numbers of DLT networks to minimum. In case of multiple DLT networks, APIs would be required for inter-operability among DLT networks. Access provider(s) establishing DLT networks would be required to share details of APIs to successfully inter operate. Regulatory Sanbdox may also be set up, if required, to test inter-operability.

Blockchain (or the broader, more generic term: Distributed Ledger Technology) is a much-hyped concept that evokes vociferous arguments, both from its supporters and detractors alike.

The response to TRAI's draft regulations to use this technology for governing commercial communication has seen arguments from both camps. We thank all responders for their comments, which have brought greater clarity to the conclusions.

The detractors have expressed the opinion that TRAI has been taken in by the hype to embrace a concept that's neither ready for adoption nor suitable for use in the manner proposed. Let's examine the broad arguments that are offered in support of such averments.

- Slow speed, lack of scalability and wasteful energy use

  The blockchain chain is a **cumbersome database that is slow and doesn't scale well**. It is also very **expensive in terms of energy use**. Therefore, blockchain should be avoided unless there are compelling reasons for its adoption.

  In the process of recording data on the system, the Distributed Ledger Technology (DLT) requires consensus to be built and maintained across multiple nodes. Compared to the conventional databases, this is indeed a slow process. It is especially slow in case of the blockchain underlying the bitcoin network because of the Proof of Work (PoW) algorithm for creating consensus. Registration of preferences or consent—or registration of entities, templates, complaints, etc. does not require speed. Some of these processes take 7 days to take effect today or are not handled at all. So speed isn't crucial in the required solution. But whatever the speed limitation of a DLT network, these pertain to writing to the ledger. Reading from it is quite fast and an in-memory database that reads from the DLT network to provide a scrubbing service (for instance) has no performance limitations.

  The PoW algorithm is required for bitcoin because there is a race among the bitcoin miners to record every new transaction. The one who has solved the set mathematical puzzle first offers his solution to the network as proof of work done and earns the right to collect any rewards associated with the transition. That makes PoW an energy intensive algorithm.

  A permissioned DLT network doesn't require PoW, so it is neither as slow nor as energy intensive.

- A permissioned DLT network isn't the real deal

  One of the advantage of blockchain technology is that it eliminates the need for a central authority, which leads to two (polar opposite) arguments against its adoption in the present case.

  The first argument is that the **TRAI could act as the Authoritative Source of information**. It is heart-warming when a stakeholder writes that TRAI can be completely trusted. However, in a centralized system, such as the one running at the moment, the authoritative server becomes a single point of failure. Furthermore, it is established by regulation, has set protocols and is too inflexible to respond to the changing needs of the sector.

  TRAI seeks to promote co-regulation and flexibility in this regulation. Retaining responsibility for an operational component is incompatible with this approach.

The second argument is that **permissioned DLT network are not fully decentralized**, which is a drawback of the proposed solution. This argument takes the other extreme viewpoint.

The telcos, the telemarketers, the principal entities (businesses like banks, insurance companies, airlines, etc.) and the subscriber are all known participants in the system. There is no role for completely untrusted elements to participate in the system or to act as endorsers for the transactions. Further, non-repudiation of previous actions is important in the solution but not some other problems, like double-spending in cryptocurrencies, that requires other features of a fully-trustless system.

In the present case, stakeholders can be allowed to record actions signed by them. A permissioned DLT network is just the right fit for this use case.

- Distributed Ledger Technology is yet untested

The **technology is new**, but it has been a long time in the making.

The Byzantine General's Problem at the heart of consensus determination has been studied in the context of fault tolerant computer system for four decades. The broader philosophical problem perhaps actually goes back to the days of the Roman Empire.

The cryptographic tools used in DLT systems have a solid mathematical background and are military grade technologies.

The same Linux Foundation which develops the operating system for enterprise computing system is behind the Hyperledger DLT. A 100 year old company, like IBM has bet billions of USD in developing its product offering in this segment. Enterprise solution providers like Oracle, SAP and Microsoft all have their own DLT offerings.

There are thousands of academic papers published in the last few years that related to distributed ledgers.

The total value of bitcoins has remained over 100 billion USD in the recent past. Ethereum's market cap is half as much, with several other currencies in the billions of dollars range. There's every reason for hackers to attack these systems, which have withstood their assault.

Therefore, it is safe to say that the technologies are well-proven, even though their new uses are just beginning to emerge.

The TRAI has determined, after careful analysis and witnessing proof of concept solutions, that this technology is indeed the appropriate "RegTech" for governing commercial communication. A scrubbing service for preferences, in conjunction with improvement in recording preference from several days to a few minutes, could be implemented using the DLT system in a few weeks. *Continued…*

IndiaCode

- Interoperability of multiple DLT networks is not possible

  The great advantage of distributed ledger technologies is that consensus is automatically built, accepted and propagated through a network of nodes. **It breaks the underlying technology if everyone has their own DLT network**. Who can be trusted in this scenario?

  The truth is that a consortium of DLT networks can publish their records to each other through request-response APIs. Each exchange of information may be broken into elementary steps that are chained together with tokens exchanged from either side.

  It would be impossible for any side to reconstruct the exchange with different data without co-operation from the other side. Further, a periodic hash of exchanged information and tokens can be published to the entire consortium making any two party cooperation infeasible.

9.6.2 Performance requirements for DLT networks for purpose of UCC eco systems could be optimized considering that it is private and permissioned network, some actions may also be carried out in near real time. Reengineering of existing processes in the chain of UCC eco systems could also be helpful to optimize the performance. As far as trust in UCC eco system is concerned, DLT systems would supplement to create trust in a system which could have been possible without DLT systems. It may also be kept in mind that DLT networks would be established, operated and maintained by access providers, or on their behalf and access providers are subjected to provisions of terms and conditions of license. Access providers may include provisions to have smart contracts and using it effectively to ensure regulatory compliance while entering into legal contract with the participating entities in the UCC eco system.

Initial Draft

## 10 International references for DLT based implementation

**10.1 Regulatory framework for DLT networks:** The adoption of DLT by regulators in other jurisdictions has mainly been in relation to the financial sector. Responses of most of regulators Internationally, mainly related to financial sector, to DLT networks thus far have been more strategic. Many regulators are in the process of creating necessary regulatory framework to consider DLT networks and other innovative technology or processes while some regulators are specifically looking to embrace DLTs for their own purposes.

**10.2 Regulators embracing DLT networks for their own purposes**: The European Commission plans to set up a FinTech task force that will look at all emerging technologies including those linked to blockchain virtual currencies. In the UK, the Government Office for Sciences published a generally positive report and recommended embracing DLT for specific purposes, describing developments as potentially catalyzing 'exceptional levels of innovation.

10.2.1 Over and above policy support for DLT development, certain regulators and governments are embracing DLT themselves. In Singapore, the MAS is fully embracing DLT in partnering with R3 and a consortium of financial institutions on a proof of concept (POC) project to conduct inter-bank payments using blockchain. The project will develop a pilot system in which blockchain infrastructure is used to issue and transfer funds among participants.

10.2.2 **Regulators enabling opportunities to test and demonstrate DLT based solutions:** Some financial regulators embracing the concept of a 'regulatory sandbox' that may allow beta testing of DLTs and

other FinTech applications. These 'sandboxes' have been created or are in the process of being created in the US, Singapore, UK, Australia, and Abu Dhabi. The UK Financial Conduct Authority (FCA) for example, has started a FinTech sandbox program, which allows a limited launch of FinTech applications, products, and services. In the US, a bill has been proposed to mandate federal support for FinTech sandboxes. In Singapore, the Monetary Authority of Singapore (MAS) recently published its FinTech regulatory sandbox guidelines. Regulatory sandboxes that allow DLTs to be tested in markets may be embraced in a familiar form to that of the 'test and learn'.

## 11 Impact of Regulations on Access Providers and the ecosystem

**11.1** Comparison with current regulations (Notified in year 2010): Obligations of access providers as per current regulations puts the burden on the access providers for doing the following:

i. Setting up of Customer Preference Registration Facility and synchronizing with the central facility maintained by TRAI in a semi-automatic or manual mode.

ii. Setting up Complaints Registration facility and handling a manual complaints resolution process including examination of complaints by verifying CDRs and disconnecting telephone connection violating UCC regulations. It also includes synchronizing the complaint related information and updates on TRAI portal

iii. Scrubbing of the commercial communication messages against preference and also scrubbing and filtering voice calls from 140-level numbers to the customers who have opted-out from receiving commercial communications

iv. Implementing signature solution and updating such solutions periodically for next threats

v. Header registration (whitelisting) and maintain records of entities to effectively handle complaints

vi. Verification of various records of registered telemarketers at the time of taking telecom resources, maintaining telemarketers' telecom resource records and to manage compliances of regulatory requirements for telemarketers

vii. Creating blacklist of telemarketers and UTMs closed for violation of the regulations

Further, the current regulation also provides for financial disincentive of up to Rs 5000 for every complaint by the subscriber of unsolicited commercial communication from an unregistered telemarketer. Such provisions have now been removed with protections built into technology solutions, thus reducing access provider's' risk and burden.

New framework is simple, technology driven, encourages automation, permits authorization/ delegation of various functions to participating entities to ensure regulatory compliance, hence reducing the burden on access providers while facilitating other stakeholders in the conduct of commercial communications as business. Deliberation in paras below clearly highlights the advantages of these regulations over current regulations.

11.2 Efficiency advantages of technology

In the years since the coming into force of the current regulation, new technologies have emerged, such as cloud computing and distributed ledgers. New challenges have also emerged, such as those from Robocalls. This has necessitated an upgrade of technology in fighting unwanted communication. Use of state of Art technology not only made the process effective, but also reduced human intervention and cost of regulatory compliances.

**11.3 Streamlining of processes**

IndiaCode

Making non-repudiable records available to relevant stakeholders allows faster, automatic resolution of issues that currently requires manual efforts. This reduces the burden of work on the access providers, minimizes likely disputes, effective complaint redressal in time bound manner, curtails chances of victimization of subscriber by wrong disconnection of telecom resources and also cost burdens on the access providers.

**11.4 The advantage of Cloud Services**

Introduction of cloud-based services for scrubbing commercial messages, handling registration of headers or managing the complaints process provides the benefits of scale compared to the current system where infrastructure is owned by stakeholders themselves, such as telemarketers. The cost advantage of cloud-based services is proven by the explosive growth of these services and widely recognized.

**11.5 A Negligible burden for implementation of regulations**

The new framework prescribed through these regulations is user friendly and automated using latest technological advancements to curb the menace of Unsolicited Commercial Communications (UCC). In this regard, the concern of few stakeholders that implementation of these regulations will have enhanced financial burden for regulatory compliance has also been analysed. It is noticed that the use of advanced technology not only smoothen various processes but also drastically reduces the compliance cost. These regulations also permit access providers to authorize DLT network operators to establish the infrastructure, operate and maintain the same which will further reduce the financial burden on access providers. Such infrastructures may also be in shared mode among access providers which would further reduce implementation and operation cost.

Technology solutions further unbundles the functions required to be performed for regulatory compliances. This opens up the opportunity for various stakeholders to consolidate infrastructure resource requirements and share resources among themselves to bring down the cost of compliance. These entities will have a business model considering large number of commercial communication messages flowing through telecom networks. In this regard, it is observed that such messages are in order of 20 to 30 billion in a month.

It is expected that cost of compliance to implement these regulations if calculated on per message basis would be minuscule while it will give flexibility to consumers to exercise various options relating to receipt of commercial communications, manage their consent effectively and also reduce the regulatory burden of the telecom service provider due to automation of processes and sharing various functions with participating entities.

**11.6 Benefits to different stakeholders:** Implementation of new regulatory framework would benefit all stakeholders.

11.6.1 **Customers would be benefited as it would:**

i. Enable capabilities in the system to define categories for preferences in more granular manner and thus allowing them to precisely convey their interest areas;

ii. Empowering them to know the scope and purpose of the consent before they give consent to the sender and requiring proper verifcation that customer has agreed to give consent;

iii. Allowing them to set their preference about types of days, time bands on which they would like to receive commercial communications. It also allows them to set preferred modes of communication;

iv. Empowering them to have more control to manage consent and preferences;

v. Implements choices exercised by them to come very quickly into force;

vi. Enables faster resolution of UCC related complaints and keep them informed about the status of resolution of complaints;

vii. Avoid inconvenience to them because of UCC from UTMs as such activities are controlled in more efficient and effective manner. Genuine communication from RTMs or senders would be displaying authenticated identities of the sender;

viii. Avoid chances of their victimization because of false complaints and protect them from disconnection of their telecom resources.

11.6.2 **Access Providers would be benefited as it would:**

i. Not levy Financial Disincentives on them on account of UCC from UTMs as they would be implementing technology driven solution to control UCC from UTMs in more efficient and effective manner;

ii. Provide flexibility to them to formulate codes of practices, agility provided by the technology solutions to quickly control participants in the UCC eco system, enhanced capabilities to function in more efficient and effective manner to enforce the envisaged provisions;

iii. Reduce regulatory burden on them as regulation permits them to authorize/ delegate various functions to participating entities to carry out regulator compliances;

iv. Provide complete flexibility to supervise and control the functioning of participating entities including passing on financial disincentives for under performance;

v. Allow them to take advantages of economy of scale as technology driven solutions provides unbundling of telemarketing functions and delegating it to the entity who is expert in that area and uses cloud-based infrastructure;

vi. Increase business opportunity to them by smoothening the processes via automation and enabling to quickly on-board the telemarketers;

vii. Provide capability to them to trace defaulting entity in case of non-compliances and take action against them as technology driven solution authenticates participating entities during operation and keeps records in immutable and non repudiable manner;

viii. Provide them opportunity to test and develop new processes using regulatory sandbox which may help them to introduce new innovative business models and may also options to introduce new ways to ensure regulatory compliances which may be implemented at lower cost;

ix. Avoid loss of business opportunities to them as it mitigates chances of victimization of its customers on account of false complaints;

x. Provide them new business opportunities as they can offer new services such as Calling Name facilities to business entities, intelligent solutions to principal entities for managing their headers for the purpose of their direct sales agents (DSAs) or authorized agents.

11.6.3 **Registered Telemarketers as it would:**

i. Provide them ease to do business as new system is very simple to get on-boarded with minimal upfront cost and quick to enter into the market;

ii. Reduce risk for them as chances of flouting of regulatory compliances would be less as robust mechanism and technology driven solutions would carry out requisite pre-checks to ensure compliances;

iii. Lower upfront cost to start telemarketing business as functions and infrastructures would be available as a service such as scrubbing as a service and additional capital & operational cost would be very less or insignificant;

iv. Avoids chances of loss of business of opportunities to UTMs because of quick detection of UTM activities and immediately putting Usage Cap on suspected UTMs;

v. Enhance volume of business due to flexible options to customers as many may like to receive such messages in their leisure time;

vi. Enhance business opportunities for them as they can participate in new functions and roles such as consent acquisition;

11.6.4 **Business entities as it would:**

i. Enhance business opportunities for them by providing better ways and means to reach out to target customers according to their interest areas;

ii. Enhance chances for them to strike the deal as they would be dealing with targeted customer base and communicating them in accordance to recipient's interest areas and their preferred timings and modes of communication;

iii. Enable to keep client data in safe and secure manner while sharing it with other entities or carrying out activities or functions required to ensure regulatory compliances;

iv. Protect their Brand as it would provide capabilities to display their identity after authentication and would also enable to display their brand name by using calling name functionality;

v. Lower risks because of avoiding chances of non-compliances by their DSAs or authorized agents as they would have better control over them by using technology driven solutions;

vi. Provide options to connect directly with the entities who are actually carrying out regulatory functions or providing resources from access providers to deliver communications and avoid unnecessary intermediaries.

InfiaCode