



Telecom Regulatory Authority of India



Consultation Paper
on
Unsolicited Commercial Communication

14th September 2017

**Mahanagar Door Sanchar Bhawan,
J.L. Nehru Marg, (Old Minto Road)
New Delhi - 110002, India**

Stakeholders are requested to send their comments, preferably in electronic form to the following address:

Shri. Asit Kadayan,
Advisor (QoS),
Telecom Regulatory Authority of India (TRAI),
Mahanagar Door Sanchar Bhawan,
J.L. Nehru Marg, (Old Minto Road)
New Delhi - 110002, India
Email: advqos@traigov.in

Last Date for submission of comments: 12th of October 2017

Last Date for submission of counter comments: 26th of October 2017

Comments will be posted on TRAI website www.traigov.in.

For any clarification/information, Advisor (QoS) may be contacted at

Tel. No.+91-11-2323-0404, Fax: +91-11-2321-3036.

Contents

1	Introduction	1
1.1	Overview	1
1.2	Key issues	3
1.3	Background	5
1.4	Recent trends	7
1.5	Summary	8
2	Customer Preference Registration System	9
2.1	Introduction	9
2.2	Analysis of present system	10
2.3	Options to make system more efficient	14
2.4	Options to make system more effective	17
2.5	New variants of unsolicited calls	18
3	Registration System for Related Entities	23
3.1	Introduction	23
3.2	Analysis of system for telemarketer	25
3.3	Analysis of system for TMSEs	29
3.4	Analysis of system for content providers	34
3.5	Options to make system more effective and efficient	36
4	UCC Complaint Handling	45
4.1	Introduction	45
4.2	Analysis of UCC complaint handling system	46
4.3	Options to make system more efficient	50
4.4	Options to make system more effective	51
4.5	Cases of false complaints	53
5	Issues for Consultation	56
	ANNEXURE-I: Key Initiatives by TRAI	62

ANNEXURE-II: International Scenario	69
ANNEXURE-III Telemarketer Statistics	73
List of Abbreviations	75
References	77

Chapter 1

Introduction

- Provides an overview of present Eco-system to deal with Unsolicited Commercial Communications (UCC).
- Provides details about approach adopted to deal with Registered Telemarketer (RTM), Transactional Message Sending Entities (TMSE) and Unregistered Telemarketer (UTM) for compliance and actions taken in case of non-compliance.
- Provides an overview of various problem areas with present system like UCC related complaints are on rise, long time taken to register or to take action against UCC complaints, victimization cases, issues of similar headers, traceability of Content Providers, consent taking process of TMSEs etc.
- Provides background of UCC regulations and key initiatives taken by TRAI to curb the UCC.
- Highlights new trends like robocalls and silent calls which may be of concern to the customers.

1.1 Overview

1.1.1 Unsolicited calls and SMS are serious problem. TRAI has taken several initiatives since year 2007 to try and protect consumers from these telemarketing calls and messages and has intervened from time to time, to control or mitigate this problem.

1.1.2 TRAI has set up a regulatory framework for subscribers to register for not getting calls and SMS from telemarketers, if one is registered with preference set as fully blocked. Provisions are also there to set one or many out of pre-defined seven categories of fields or

areas in which one may be interested to receive telemarketer SMS, but such SMS should not come for rest of the categories.

1.1.3 TRAI has launched an app that helps to detect and report spam, and a large database of spam numbers based on crowd-sourcing is also being developed. In addition to regulatory intervention, manufacturers and service providers are also offering various options to help block such callers on a smartphone.

1.1.4 Telemarketing activities are permitted only after registration with TRAI and after entering into agreements with Telecom Service Providers (TSP). There are different standard agreements for different purposes e.g. for promotional voice calls, promotional SMS, transactional SMS, SMS with reply, etc. and also telecom resources are segregated for different purposes.

1.1.5 To identify, source of telemarketing messages and voice calls from registered telemarketers and content providers, identifiers, headers and dedicated levels are assigned. To know the TSP and License Service Area (LSA) from which registered telemarketer (RTM) has taken connectivity to deliver the messages or call the customer, predefined prefixes have to be inserted. This helps to trace the route of telemarketing SMS or voice call. For detecting telemarketing SMS from Unregistered Telemarketers (UTMs), which is not allowed, telecom service providers (TSPs) were asked to deploy signature solutions that attempt to identify UTMs and block unauthorized messages by matching the content and/or number pattern.

1.1.6 In case registered telemarketers do not comply with the registered preferences of the customers, they have to pay, by way of financial disincentives, through deductions from security deposits made at the time of registration. In case of repeated non-compliance beyond a threshold or non-availability of sufficient security deposit, RTMs are black listed for two years and telecom resources allocated to them are withdrawn.

1.1.7 If in case it is found that the UCC was sent by an UTM, i.e. a ten-digit number then that number is disconnected and the concerned person's name is black listed. This blacklisting leads to the disconnection of other telecom resources belonging to same person.

1.1.8 Earlier, it was also noticed that a large number of complaints received from consumers pertain to calls or messages originated by or on behalf of banks, insurance companies, builders etc. who are promoting their business by engaging unregistered telemarketers in total disregard of the regulations made by the Authority. These organisations, being the principal are equally responsible for the non-compliance of the regulations and directions issued by

the Authority to address the problem of UCC. It is the responsibility of these organisations (the principals) to ensure that the telemarketer engaged by them (the agent) for promoting their business either directly or through an intermediary follows all rules and regulations and if such organisation (the agent) fails in this responsibility, they (the principals) are to be held responsible for the acts and omissions of their agents. Hence, in order to make these entities accountable, regulations were amended to provide provisions for disconnection of all telecom resources of such organisations if they are found to be engaged in telemarketing through unregistered telemarketers. At that time it was viewed that the disconnection of the principal entity's telecom resources will act as a deterrent and inculcate a greater sense of responsibility in these organisations.

1.2 Key issues

1.2.1 From complaints being received on regular basis and feedback from various sources, it is evident that problem of Unsolicited Commercial Communication (UCC) is far from being under control. Though telemarketing voice calls from RTMs are largely controlled, unsolicited SMSs still persists and many customers who have registered their preference not to receive such SMS are still getting them. UCC calls and SMS from ten-digit number or UTMs too are still a problem, despite disconnection of large telephone numbers. Unscrupulous elements are able to manage new connections and continue to indulge in these activities. Therefore, there is a need to devise a mechanism which is more effective in dealing with these issues.

1.2.2 Incidences have come to notice where it is found that their agents are not complying with provisions of UCC regulation. However, these entities express inability to keep tabs on agents which are sending unauthorized messages or making calls related to promotion of business or commercial offerings of principal entity. In such cases, they file a complaint with police, but in almost all cases it does not result into any action as they are not traceable.

1.2.3 With present regulatory provisions and processes in place, it takes seven days for the preferences registered by the customer to become effective. With current technology solutions, it should be possible to update the records at necessary places and enforce the preference in much less time. Similarly, the time for resolution of a complaint may also be shortened and thus the time window available with the UTMs before an action is taken can be reduced substantially.

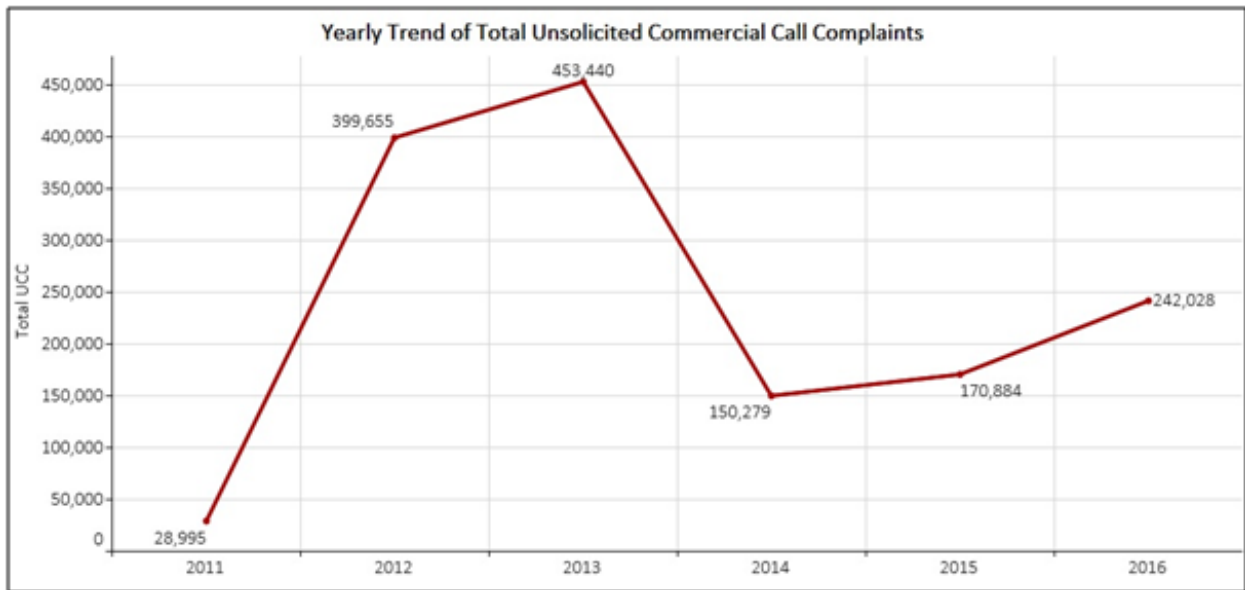


Figure 1.1: Year-wise trend of UCC Complaints

1.2.4 Disconnection of UTMs, on the basis of complaints of single person may affect the other person adversely. Cases have also been observed where Customer Acquisition Form (CAF) against a UTM number was fake and that may also lead to disconnection of telecom resources of a person who is not guilty at all. Such false complaints in recent times, are seen even when the parties had a commercial or business relationship between them.

1.2.5 Present mechanism, does not have necessary ways and means to protect the data that are made available to the registered telemarketers. Protecting this data may limit the exploitation by UTMs to certain extent as chances of falling that data into hands of unscrupulous elements gets reduced. In such protection system customers who are not registered(i.e whose complaints presently are not handled) couldn't be targetted.

1.2.6 Earlier, these calls and messages were simply annoying while nowadays, they are also being used by scammers trying to steal the identity or mislead the target for making some investments. Recently, SEBI and RBI have approached TRAI for help in controlling misuse by unscrupulous elements who send unauthorized investment tips or misguide in some ways. Traceability of such miscreants is also a big 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. This requires signature solution to detect traffic from RTMs in addition to detecting patterns in traffic from UTMs.

1.2.7 It has also come to notice that there are a number of intermediaries between registered telemarketers and content providers. At present, there is no standard agreement between registered telemarketers (RTMs) and content providers or intermediaries. It also results into non-traceability of culprit in case there is a misuse of transactional pipe by the content provider. Misuse may be temporary or regular in nature and may involve mixing of transactional & promotional text or sending misleading advice etc. However, RTMs taken telecom resources from Access Providers may be responsible to check such misuses but there may be difficulty in detecting as content of transactional pipe may be required to be screened and compared with reference template, either by the RTM or by the TSP. There may be a need to devise a mechanism which is capable to addresses the problem for large number of content provider entities and large volume of traffic.

1.2.8 Present regulation permits registered companies to send communication to its clients related to goods and services, which is not promotional in nature. Such companies are supposed to take consent from the client which is verifiable and renew the consent periodically. However, it is found that in practice, telephone numbers of customers are collected at the time of purchase of item or taking services and in most of the cases, customer is not aware about the implications of sharing of number. He starts getting messages or calls related to the goods and services including new offers. At present, there is no robust mechanism to keep the record of consent which is non-repudiable and accessible to resolve the complaint quickly.

1.2.9 TSPs have represented that they have deployed signature solution and most of the time they are taking action against UTMs within stipulated time, even then they are being asked to pay by way of financial disincentives. They argue that they should not be made responsible for the act which they have not done or they are not responsible for. It is required to revisit role and responsibilities of TSPs and to take a relook into the present provisions in the regulations related to financial disincentives.

1.2.10 In view of above and many other aspects which are detailed in subsequent chapters, regulatory framework for UCC is required to be reviewed for appropriate changes in the framework or for introducing new entities or processes required, if any.

1.3 Background

1.3.1 Key entities of the "Telecom Commercial Communication Customer Preference Regulation, 2010" [7] and known as TCCCPR, 2010 are illustrated in the figure 1.2.

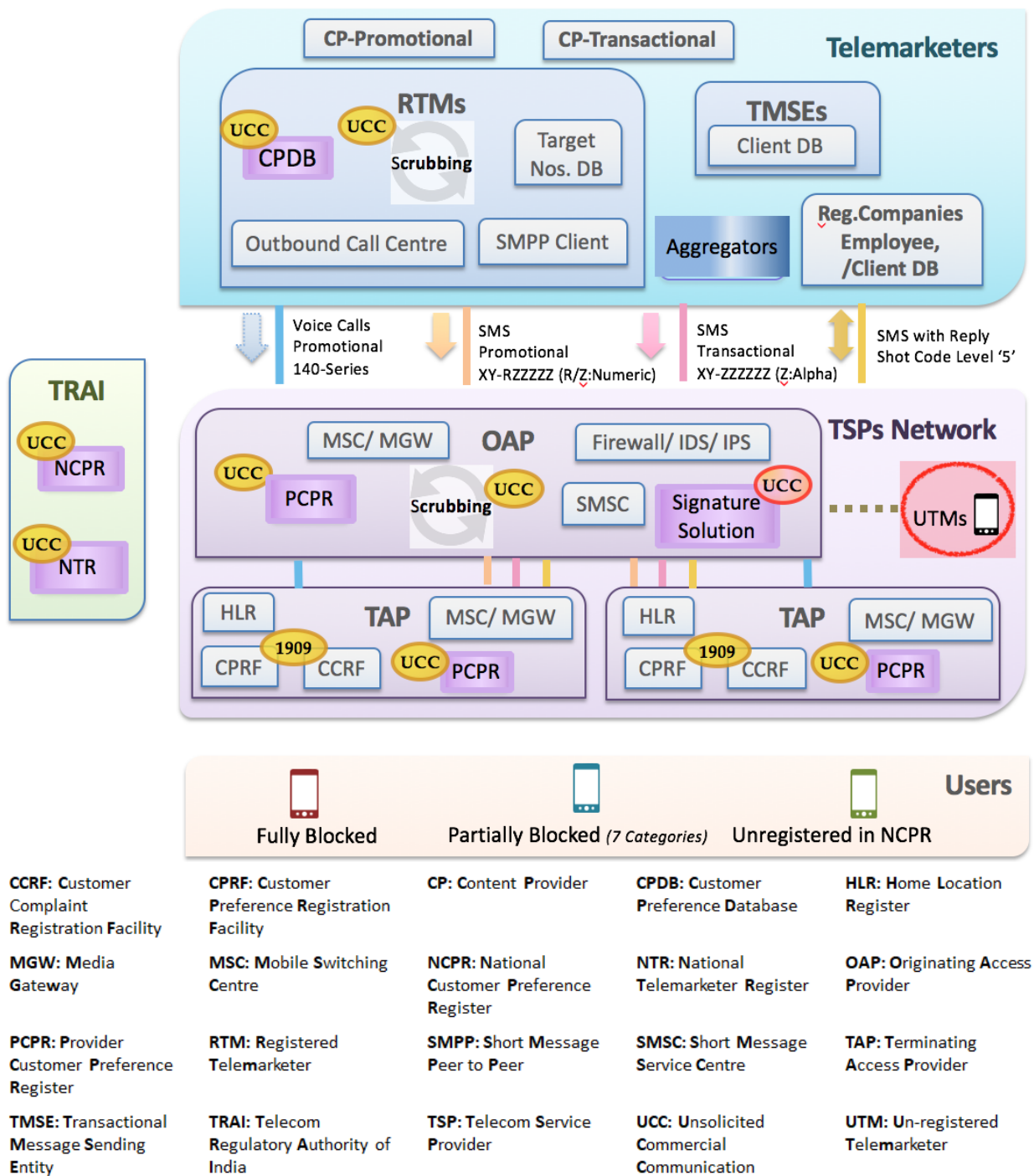


Figure 1.2: Present UCC Ecosystem

1.3.2 Unsolicited Commercial Communication are being regulated with principal regulation TCCCPR-2010. This regulation has gone through sixteen amendments. This regulation has provision for Customer Preference Registration Facility (CPRF), Provider & National Customer Preference Registers (PCPR & NCPR), National Telemarketer Register (NTR). It also prescribes registration procedure for Customer Preference and Telemarketer registration. Obligations of Telecom Service Provider (TSP), blacklisting of telemarketers and subscribers found sending Unsolicited Commercial Communication (UCC) are also prescribed in this. There are seven schedules to this regulation which includes procedure for registration of preference, telemarketer, standard agreement between TSP and RTMs, Transactional Message Sending Entities (TMSEs).

1.3.3 Key initiatives taken by TRAI to curb UCC are listed in the Annexure-I to this consultation paper. Further details regarding regulation and the subsequent amendments are available at <http://traai.gov.in/release-publication/regulations/amendments-page/88235>.

1.4 Recent trends

1.4.1 Recently telemarketing calls are also using auto-dialers to deliver a pre-recorded message and also making calls using capabilities of latest technologies which make automated calls as if from a robot. These calls may also be interactive. Robocalls are often associated with telemarketing phone campaigns, but can also be used for public-service or emergency announcements. Some robocalls use personalized audio messages to simulate an actual personal phone call. Robocallers are exploiting advancements in technologies e.g. computerized auto-dialers, text-to-speech, speech-to-text, cloud based call centre etc. Large scale operations with lower costs and support of multi-lingual, interactive, personalized calls are also being exploited by scammers and spammers.

1.4.2 Another trend in telemarketing calls is being seen through silent calls. In this case, one may find occurrence of a call in the missed calls log which had no any ring or alert like other normal calls. When, one tries to call back on same number he hear an information message or promotional offer from the organization which was calling. In such cases, handling of complaints of UCC, may not find any evidence of call made by the organization to the person as it was silent call and was not picked up. In fact, from Call Detail Records (CDR), it will be seen as person contacted organization as CDR of calling back to the silent number is generated.

1.5 Summary

It is obvious from discussions in para(s) above that there is need to re-look into the current framework of regulations for UCC. Issues are deliberated in more detailed manner in next three chapters.

1.5.1 Chapter 2 deals with the Customer Preference Registration System. It analyses present preference registration system and attempts as to how to make system more effective and efficient. It also deliberates options to provide more choices to the customer for preferences.

1.5.2 Chapter 3 deals with the Registration System for related entities. It analyses present registration system for Telemarketers. It explores possibility of registration of new entities like Content Providers, Aggregators, Intermediaries. It also suggests introducing new entities for Header Assignments, consent recording etc. Ways and methods to verify content sent by content provider is also deliberated in the chapter.

1.5.3 Chapter 4 deals with the issues related to UCC Complaint handling. It analyses UCC complaint handling procedure in the present system and also attempts to make the system more efficient by reducing time-line through scrubbing as a service. The chapter also explores options such as enhanced functionality of signature solution, introduction of honeypots etc to make the system more effective.

1.5.4 Finally, all the issues for consultation raised in the respective chapters are summarized in Chapter 5 and seeks suggestions and inputs from all the stakeholders.

Chapter 2

Customer Preference Registration System

- Highlights difficulties faced by customer in getting registered. Introduces usefulness of channels like Mobile App and Web portal as an effective tool to get registered with better success rate. It also Explores options for feature phone customers to provide similar type of capabilities e.g. USSD. It also explores ways and means to improve penetration and adoption of TRAI Mobile App.
- It suggests ways to reduce time required to register and enforce keeping in view the availability of latest technology platforms and solutions like cloud based platforms for hosting application and data, options to provide Scrubbing as a Service, options to introduce process of bulk registration.
- It suggests to introduce more categories, sub-categories for preferences and also new choice types such as media type, preferred day and time.
- It suggests to provide better experience for customers during Mobile Number Portability by retaining preference registrations of customers.

2.1 Introduction

2.1.1 In the present system, Customer Preference Registration Facility (CPRF) is provided by Access providers (APs), for registration or de-registration of their preference regarding receipt of commercial communication and it is accessible by a short code 1909 which is toll-free. Every access provider maintains and operates Provider Customer Preference Register (PCPR) for registering the preference of the subscriber as fully blocked or partially blocked

category. Every PCPR, inter-alia includes:

- a. the name of each subscriber who makes a request to the Access Provider indicating his preference
- b. telephone number of the subscriber including area code in case of wireline
- c. the date and time of the request by the subscriber
- d. the details of the preference made by the subscriber
- e. the unique registration number (URN)

2.1.2 For keeping central repository of preferences registered by all the customers across all Access Providers, National Customer Preference Register (NCPR)[6] is established and maintained by the Authority. NCPR contains the telephone number and details of preference of subscribers who have registered themselves.

2.1.3 Procedure for registration of preference by a customer is specified in Schedule-I of the regulation. Every Access Provider, immediately on receipt of a request verifies the correctness of the request so received and communicates, through SMS, within 24 hours of the request, a unique registration number (URN) to the subscriber.

2.1.4 Any subscriber may, at any time after expiry of seven days from the date of registration or seven days from date of last change of his request, change his preference. Access Provider verifies the correctness of the request and confirms the same, within 24 hours, to the subscriber through SMS. Any subscriber, after expiry of 3 months from the date of registration, can request for withdrawal of his registration. The Access Provider within 24 hours of the receipt of request, verifies the correctness of the request and deletes the telephone number of the subscriber from the PCPR and confirm the same, within 24 hours, to the subscriber through SMS. Access Provider, within 24 hours of registration, or a change or de-registration, updates the NCPR.

2.1.5 The process of registration of preference or change of preference or de-registration is illustrated in figure 2.1. The figure illustrates various entities involved in the registration process and maximum time frame specified in the regulation to perform the activity.

2.2 Analysis of present system

2.2.1 In the present system, the customer of a service provider can register its preference regarding commercial communication through various methods such as calling to call centre

or IVRS, through SMS, e-mail, web based application or mobile App. Based on the customer preference two types of registers namely Providers Customer Preference Register (PCPR) and National Customer Preference Register (NCPR) are updated. The regulations provide specific time-frame for updating these registers and enforcing the customers preference within seven days from the date of registration of the preference. The time of seven days seems to be quite high considering the latest technology solutions which are available now-a-days in the IT field. To achieve reduction in time frame for registration, one of the aspects may be to automate the process at every node involved in the registration process and other aspect may be to specify the procedure to communicate between nodes.

2.2.2 Analysis of the current process being adopted indicates another issue that the system is not user friendly and many a time customers are not able to register their preferences in spite of availability of various options to register their preferences. Many customers are either not aware of the call centre number to register their preference or find uncomfortable to register through use of IVRS. Many service providers, before connecting to call centre executive, asks to select various options in the IVRS prompts and then only customer can interact for registration of preference. As a result, though the framework has been prescribed, it is not being effectively used by the masses and there is a need to address this issue.

2.2.3 Further other mediums than IVRS like SMS, email, and web based application are also complex from user prospective. It expects that the customer is familiar with the details of the parameters to be send for the registration of his preference and that too in a given sequence. If the information is not provided in a structured manner, then it is not considered as valid and customer request for registration of preference is not accepted. It may require to identify the modes or channels of registration which may increase the probability of getting registered in first attempt and promote these channels over other ones.

2.2.4 It is also observed that present registration system requires registration of every individual one by one, even when all individuals belong to same family or organization. It leads to requirements that every individual must be acquainted with the process of registration and spare time for this purpose. In some cases, bulk registration may help to effectively reduce registration time by providing enbloc registration or allowing to carry out other person on their behalf. Such facility is likely to enhance the count of customers registered on NCPR.

2.2.5 The other issue of concern relates to instances of customer getting de-registered during mobile number portability process. Many a time customer is not aware about it and continues to suffer for long time. The analysis reveals that during mobile number portability process,

donor network is initiating UCC de-registration of customer, if customer was registered with NCPR and recipient network initiates the registration process for UCC only after getting fresh requests from customer. This not only results in increasing system load for de-registration and registration unnecessarily but also creates additional burden on customer to re-register again. At present, no specific provision has been made in the regulations to deal with cases of mobile number portability. It is also observed that in case, there is delay in de-registration of customer preference from donor network side and it is triggered after registration request initiated by recipient network then it may happen that final state of customer may get recorded as de-registered in spite of the fact that customer has re-registered after mobile number portability. It needs to specify the sequence and timeline for registration or de-registration process during the MNP process. One may also argue that the status of customer preference remain unchanged during MNP as it does not impact customer preference.

2.2.6 Another issue relates to the closure and reassignment of the telephone number. In the present system there is no process to differentiate between telephone number and customer in the NCPR records. For example, if record corresponding to a telephone number is retrieved from NCPR, it may indicate details about registration, de-registration, re-registration of telephone number including even that period during which telephone number was not in the name of current customer. This may happen when number was closed and re-opened in the name of another person after certain period. Both capabilities may be required, retrieval of records against a customer and against customer identity. This may require to specify the procedure during closure of service or during transfer of phone in another name.

2.2.7 The present regulatory framework prescribed options for the fully blocked category and partially blocked category. While both voice calls and SMSs from telemarketers are blocked in fully blocked category, customer has option in partially blocked category to choose to get SMS from seven categories of entities at the time of customer preference registration though voice call will be completely blocked from any telemarketers. These categories are quite broad and cover very large area. Individual may not be interested in all the messages belonging to these broad categories and choosing particular category may leave him annoyed in most of the cases. In view of this, there may be a need to provide options for additional categories of preferences.

2.3 Options to make system more efficient

2.3.1 To achieve reduction in time lines for registration and its enforcement, first and foremost requirement is that all nodes involved in the registration and enforcement process are available 24X7. Nodes at Access Provider side and TRAI side e.g. CPRF, PCPR, NCPR etc. are available 24X7 and have redundancy but nodes involved at RTM side may not be having same level of availability. In fact, there may be lot of variations in the capabilities of the systems used at RTM end. Constraints even at one node, may make difficult to achieve reduction in time lines. One of the option may be to avoid the requirement of periodic download of NCPR data by the RTMs and then ask RTMs to upload the data of target numbers along with type of communication to be made for telemarketing purpose to a cloud based platform. The cloud based platform may thus provide Scrubbing as a Service which may return the list of numbers that may be allowed for the purpose specified. This approach may eliminate the need for RTMs to have system which is available 24X7 as they will be provided list of numbers which may be contacted as per the latest data. Keeping in view the broadband connection availability and cloud based platform which can scale up and provide reliable Scrubbing as a Service seems to be a feasible option. However, this may require to identify the agency which will provide such services on charge basis. One of the option may be that this is operated and maintained by a consortium of access providers under supervision of TRAI. Charges may be based on multiple factors e.g. number of records, number of accounts, account duration based.

2.3.2 In France, telemarketer submits a list of the prospective persons to be solicited, and the operator sends back the list with the numbers registered in the system deleted.[3] However, there may be requirement to prescribe fixed charges or maximum charges for availing such services. The charges may be dependent upon various factors like size of the list, frequency at which services are accessed, performance requirements etc.

2.3.3 To reduce time line, another important requirement is to automate the process at every node and run it real time or near-real time. For example, at present communication between PCPR and NCPR involves MS Excel file or CSV file upload and download. Script is run on regular basis on the nodes to update the database from files received till that time and to generate the output files from the updated database. Instead of this, use of APIs may be helpful to carry out update as soon as new request for registration or change is received. In addition to this, standard operating procedure may be helpful to automate actions at every node and avoid human intervention. In order to automate the process at the first point of interface i.e. Customer Preference Resource Functionality (CPRF), availability of

structured data during registration request may be an essential requirement.

2.3.4 For ensuring that all relevant information is available in the request received from the customer, there is a need to analyze the type of channels used for registration. For this purpose, channels of customer Preference Registration Facility (CPRF) may be categorized into two types, first type of channels which are structured and submit validated requests for registration. Another type of channel which are unstructured & do not validate the requests before submission. For example in case of mobile apps or web portals, request form may be structured and validated, to certain extent, before submission of the request by the customer and there is a high probability that preferences are registered in first attempt. However, for unstructured communications, not much can be done but there may be option to explore to switch customer from unstructured to structured channel type e.g. if somebody submits incomplete information in the SMS template then he may be provided link to an interactive mobile site for CPRF registration or network initiated USSD session. This approach may be helpful to make registration process more user friendly and also improve the chances of getting registered in the first attempt. Therefore there is a need to promote first type of channels and make it available for wider cross-section of the users.

2.3.5 Mobile app, which belong to first type of channels for registration, can be one of the most effective methods to enhance customer interaction with the service providers be it for all types of activities e.g. the registration of the preference, changing of preferences or checking the status of the registration or de-registration etc. Capabilities of Mobile App can be enhanced even to register the complaints and it can be made available to a wider cross section of the customers. Enhancements may include automatic retrieval of current status of the customer, presenting various options to customers to choose from during inputting the request form and automatically sending it to concerned service providers. This will also reduce efforts for consumer education which are otherwise very cumbersome considering wide spread customer base. Such mobile app must be available on most of the device platforms and adopt consumer friendly installations on the devices to make it available to wider cross-section of the customers. One of the option may be to consider to make them a white label App which can be bundled with other Apps such as Mobile Apps of TSPs. TSPs can also popularize these Mobile Apps through SMS blasts, advertisements, referring to features of these apps and easy availability to download in their advertisements.

2.3.6 Therefore, there is a need to enhance various options of structured communication to register the preference by the customers. USSD may also be included as one of the options for structured communication for registration of the preference. In case of web portal, One

Time Password (OTP) type of solutions may be helpful to authenticate that the request is from genuine source.

2.3.7 Other options could be to prescribe templates for receiving customer preferences through several other modes like sending SMS, email etc. to increase registration correctly. While prescribing templates this may be helpful to some extent but people may not be comfortable to use these templates when they are using it first time and little variations may lead to rejection of the requests. Other possibility could be to explore options to switch from unstructured mode to structured mode after receiving request from the subscriber first time even if it is not in correct format. For example, if a SMS or email is received to register for UCC which is not having complete information then USSD session may be initiated or link to web portal may be sent to complete the request. This will require initiative from the telecom service providers and may also require additional expenditure to facilitate registration of customer preferences on continued basis. But on other hand it may reduce number of repeated failed attempts on a toll free Customer Preference Resource Functionality (CPRF). In view of various available options to encourage customer preference registrations, we may seek the comments of stakeholders to move forward.

2.3.8 One of the solution to enable representative of an organization or family to register preferences on their behalf is to permit preference registration in bulk. Provision for bulk registration exists in Australia where a consumer can register preferences on behalf of family members, as well as an organization etc.[2] There may be various methods and procedures for bulk registration of customer preference e.g. on line mode, off line mode. There may be limit on maximum number of registrations which can be done by one person on behalf of others which may depend upon type of mode, type of documents which are submitted, family member or an authorized signatory of an organization etc. Bulk registration may also be done through web portal and may require additional set of documents. For example, in case of registration of business/ government numbers, eligibility for bulk application may be account holder authorized for this particular purpose, nominee with evidences in form of declarations, letter from organization, certified copies of power of attorney etc. Bulk registration application may have to adhere to certain formats like file format specification, validity of format & ranges of specified numbers, restrictions to preferred choices in category for individual numbers etc. Such type of restrictions helps to facilitate automatic handling of such requests by the system. Some limit may also be required to be put in such cases for example, for registration of family numbers (not more than 5 (say) and with proper verification process).

2.3.9 For issue related to MNP, there is a need to clearly define customer preference registration handling during mobile number portability process. One of the option may be to retain the customer preferences in NCPR as it is i.e. neither de-registering nor re-registering the preferences. Other option may be to take the consent of customer for de-registration at the time of porting process but default option may be to continue with the previous state of registration. Location Routing Number (LRN) which is assigned to each TSP for MNP purposes may be recorded as a part of NCPR record for the customer. It may help to segregate NCPR data, License Service Area (LSA) wise or TSP wise.

2.3.10 For cases of closure of services, customer may need to be de-registered and telephone number may need to be tagged as closed in NCPR. It may be helpful for differentiating between history of customer and history of telephone number in cases of re-allocation of telephone number.

2.4 Options to make system more effective

2.4.1 For providing additional choices to the customer, more categories may be introduced which are relatively narrow than present categories of preferences. Following may be examples of additional categories:

- a. Agriculture, Forestry, Fishing
- b. Advertisement, Marketing, Public Relation
- c. Administrative, Support Services
- d. Architectural Services
- e. Arts, Entertainment and Media
- f. Biotechnology and Pharmaceutical
- g. Community, Social Services and NGOs
- h. Computer Hardware, Software
- i. Construction, Mining and Trades
- j. Consulting Services
- k. Employment Placement Agencies
- l. Accounts, Auditing

2.4.2 Also sub-categories may be introduced which are defined for more specific purpose in that category. For example, if banking option is chosen then one will start getting all sort of messages from all types of banks in which one may not be interested. So, if there is option for MyBank(s) then problem can be alleviated. Similarly, one may not be interested in all kinds of banking products e.g. Home loan, personal loan, car loan, investments etc. Capability to

restrict the entity or type of entities which can send messages and purpose for which they can send messages may help to reduce the gap between interest area of the customer and permitted area to RTMs for reaching to the customer. At present, scrubbing capabilities available at RTM and Access Provider end may not be sufficient to deal with increased number of categories and sub-categories and may require upgradation. Alternatively, latest technology platforms which may provide this as a service may likely help in dealing with complexity and scalability of the problem.

2.4.3 It is also felt that annoyance or irritation from different types of media e.g. voice calls, SMS, auto-dialer calls etc depends upon users choice. One may be Okay with SMS while may be uncomfortable with commercial voice calls. Media type which is used to deliver commercial communication may also matter to the customer. For example, intrusiveness of voice call may be more than a SMS as content of SMS may be seen by the customer at later convenient time while voice call usually pushes the called party to respond at the time of call. Sometimes person feels more irritated in cases of call made by an auto-dialer with pre-recorded announcement or robo-calls. There may be requirement to classify such calls as a separate category of media and offer option to customer to choose. There may also be requirement for RTMs or TMSEs to declare use of auto-diallers or rob-calls and operate in accordance to the provisions. At present, there is no option to choose preference of media for commercial communication. Preference registration may require addition of options for choosing preferred media as well. Similarly, preferred time-slots or days may also be helpful to meet both objectives, one of not disturbing during days, time-slots or through media which is not of choice of customer and same time providing options to communicate for RTMs or TMSEs with him in accordance to one's preferred choice.

2.5 New variants of unsolicited calls

2.5.1 Robocalls

i. In many countries robocall, a new variant of telemarketing call has been observed. Robocall is a phone call that uses auto-dialer to deliver a pre-recorded message, as if from a robot. Robocalls are often associated with political and telemarketing phone campaigns, but can also be used for public-service or emergency announcements. Some robocalls use personalized audio messages to simulate an actual personal phone call. Robocallers are exploiting advancements in technologies e.g. computerized auto-dialers, text-to-speech, speech-to-text, cloud based call centre etc. Using these technologies, they can scale-up to a very large target base which may be many times than that could have been possible with the person based

calling approach. With advancement of technology, they can convert text-to-speech in multiple languages including regional languages and with accent of voice of region where called party belongs to.

ii. In this way, telemarketers can reach to the different parts of a country or globe and communicate with called party in voice accent used in that region. Concatenation of pre-recorded voice with variable text-to-speech can offer a personalized or customized service and speech-to-text, phone keys etc. makes robocalls more interactive. The characteristics of robocalls are making them preferred choice for telemarketers. Now, telemarketers can handle large volumes. Cloud based call centres provide capability to scale-up their hardware capabilities up to their requirements in no time and with relatively lower capital and operational expenditures.

iii. On the other hand large scale operations with lower costs and support of multi-lingual, interactive, personalized calls are also being exploited by scammers and spammers. Robocalls because of their capabilities to reach large number of subscribers in different parts of areas in very short time have enabled to reach to persons who are vulnerable to such scams. In last few years, various scams using robocalls like lucky winner scam, 'can you hear me' scams[4], Internal Revenue Services (IRS) Scam, Tech Support Scam etc. have been identified.

iv. Usually, these are impostor scams where they can misled the caller to believe that call is from authentic and authorized sources. Caller Identity spoofing specially in VoIP calls and in case when one of the network operator interconnected with SS#7 located any where in the world has not ensured the correctness of Caller Identity may bring whole system vulnerable as it may be quite easily possible to spoof the identity. Once the caller believe then they offer some kind of offers for services for which they get transferred money from the caller out of fear or by luring them for tantalizing opportunities. In UK, in case phone spoofing or targeted by scam, there is a provision to call Action Fraud which is UK's national reporting center for fraud and internet crimes.

v. In case of "Can you hear me?" scam, the voice of caller with response of "YES" is recorded which is later used for various purposes like purchase of goods and services. In US, the service provider are urged to provide robust robocall blocking service. Such type of service offering may also help the customer combat robocalls. One type of difficulty in enforcement of illegal robocalls is that the sources of the robocalls may be from other jurisdictions. For example in Internal Revenue Services (IRS) scam in US, some indian call centres were alleged. In such type of cases, there is a need to fight against illegal robocalls through international collaboration and cooperation.

2.5.2 Silent Calls

i. One of the recent trend in telemarketing calls is silent calls. In this type of case, one may find that there was a call in the missed calls logs while no ringing or alert was noticed. When, one tries to call back on same number he hear an information message or promotional offer from the organization which was calling. In such cases, handling of complaints of UCC, may not find any evidence of call made by the organization to the person as it was silent call and was not picked up. In fact, from Call Detail Records (CDR), it will be seen as person contacted organization as CDR of calling back to the silent number is generated.

ii. Such silent calls are more observed in cases of auto-dialers and this is also done to maximize the amount of time call centre agents to spend most of the time to talk with persons who have responded rather than waiting during the ringing phase of the call. These auto dialers, dial numbers automatically and connect the person to call centre agent as soon as it is found that called person has answered. Silent calls may also be generated when numbers of call dialed are much higher than the number of call centre agents and at the time, when called party responds it may happen that there is no call centre agent free to attend the call.

iii. Silent calls can be very annoying and inconvenient to the customer especially when someone is repeatedly getting silent calls. Calling back to number appeared on silent call may also be premium rate number and may lead to charging to the customer on higher rate than a normal rate. In UK, Ofcom continually monitors complaints about abandoned and silent calls and can launch an investigation if it believes a caller is not following the law and may take enforcement action, including fining the caller up to £2 million.[5]

2.5.3 Robocalls and Silent calls may be originated from other countries and to address the issue may require International co-operation and collaboration. There may be requirement to identify the source of UCC calls originated from international locations and take action in coordinated manner. There may also be need to explore technical solutions which can be deployed at international gateways to filter out such calls.

2.5.4 Fraudster Calls or SMS

i. There are increasing trend of using SMS and voice calls for purposes of frauds, malicious, obnoxious, threatening etc. Recently SEBI and RBI have raised concerns about misleading the customers e.g. about financial investments using SMS. There are cases of SMS being sent for fake lottery awards. Some of the countries have established separate unit to deal

with such type of cases. In some cases, they may not be commercial communications as such but it may be a matter of great concern to a customer. Some calls or messages are used for malicious or obnoxious purposes and may be targeted to a particular person or group of persons.

ii. There are certain messages or calls which may be unsolicited for a customer but not a commercial communication as such. For example, daily thoughts, political party messages, market survey etc. Some countries have specifically included or excluded such types of communications under unsolicited communications.

In view of above analysis and options which may be used to make customer preference registration system more efficient and effective, suggestions and inputs of stakeholders are sought on following

Q. 1. To what extent, time required for registration and enforcement can be reduced? For achieving reduced time lines, what changes in processes or in different entities e.g. PCPR, NCPR, CPDB may be required? Will providing scrubbing as a service for RTM reduces time? Please give your suggestions with reasons.

Q. 2. How to ensure availability of Mobile Apps for registering preferences and complaints and for de-registration for all types of devices, operating systems and platforms? Whether white label TRAI Mobile App may be bundled along with other Apps or pre-installed with mobile devices for increasing penetration of app? For popularizing this app, what other initiatives can be taken? Please give your suggestions with reasons.

Q. 3. In case of Mobile Number Portability (MNP), what process may be defined for retaining the status of customer for preference registration? Please give your suggestions with reasons.

Q. 4. How bulk registration may be allowed and what may be the process and documents to register in bulk on behalf of an organization or family? Please give your suggestions with reasons.

Q. 5. Is there a need to have more granularity in the choices to actually capture customers interest and additional dimensions of preferences like type of day, me-

dia type(s)? What will be impact of additional choices of preferences on various entities like CPRF, PCPR, NCPR, CPDB etc.? Please give your suggestions with reasons.

Q. 6. Should the scope of UCC regulation be enhanced to include unwanted calls like silent, obnoxious, threatening calls etc. and unauthorized communications.? What role government or constitutional organizations may play in curbing such activities? Please give your suggestions with reasons.

Q. 7. What steps may be taken to address the issues arising from robo-calls and silent calls? What are the technical solutions available to deal with the issue? How international co-operation and collaboration may be helpful to address the issue? Please give your suggestions with reasons.

Chapter 3

Registration System for Related Entities

- Highlights the issue of inability to trace Registered Telemarketers, Content Providers and clearly demarcate roles and responsibilities among various stakeholders in the value chain.
- It examines option to register entities like aggregators, intermediaries, content providers and define obligations for each entity.
- It examines options to record customer's consent in an immutable and non-repudiable manner. It also proposes to establish central repository of headers, prescribe procedures for assignment or de-assignment of headers with allocation principles, manage life cycle of headers in various scenarios.
- It also examines need for providing option for RTMs or TMSEs to reach customers via voice calls for well justified and legitimate purposes. It also proposes to introduce robust mechanism to identify voice calls from particular organization e.g. by allocating dedicated number series, by using Intelligent Network based solutions.

3.1 Introduction

3.1.1 For registration of telemarketers in the present system, a National Telemarketer Register (NTR) is established and maintained by the Authority. It contains the details of the telemarketer such as registration date, application number and registration number. It also contains the details of the fees deposited, the number of notices for sending UCC, along with the date of such notices. And also details of blacklisting of telemarketers and the date of

blacklisting of the Unregistered Telemarketers (UTMs).

3.1.2 Schedule-III of the regulation provides procedure and conditions for the telemarketer to submit requisite documents and obtain registration number. The registration is valid for a period of five years unless revoked earlier and it may be renewed 60 days before the expiry of its registration.

3.1.3 RTM may take telecom resources from one or more Access Providers. RTM has to apply for it and submit all necessary details accompanied by Customer Acquisition Form (CAF).

3.1.4 For obtaining telecom resources, access provider has to verify that the details in application furnished by the telemarketer are correct and the registration number issued by TRAI is included. The access providers also check compliance with the subscriber verification guidelines issued by DoT and also ensure that the telecom resources are not allocated to a blacklisted telemarketer.

3.1.5 RTM has to enter into agreement with access provider at the time of taking telecom resources. Standard format for agreements are given in various schedules of the regulation. Schedule-IV is an agreement for RTMs for the purpose of promotional message, Schedule-V is an agreement for RTMs or TMSEs the purpose of sending transactional message and Schedule VII is an agreement for RTMs or TMSEs intending to receive reply from the recipient of the transactional message, in response to the transactional message sent by him.

3.1.6 Access provider before activating any telecom resources provided to a telemarketer, ensures that details of all telecom resources are entered into the NTR.

3.1.7 Every access provider has to ensure that telecom resources for

- a. making voice calls do not have facility for receiving incoming call and sending of SMS.
- b. sending transactional messages do not have facility for receiving incoming call or SMS.
- c. receiving incoming SMS, who enters into an agreement as specified in Schedule VII.

3.1.8 NTR inter alia include a blacklist of telemarketers and a blacklist of subscribers. The Name and address of a telemarketer to be entered into the black list upon:

- Failure to furnish the additional security amount as agreed by it into with the OAP
- upon service of the 6th notice in a calendar year by any Access Provider, on such telemarketer for sending UCC.

3.1.9 If the name and address of a subscriber is entered into the blacklist of subscriber then it is not to be deleted before completion of two years from the entry in the respective registers. The name and address of such telemarketers or subscribers is communicated to all access providers. Access provider on receipt of intimation, within 24 hours, have to disconnect all the telecom resources provided to the subscriber or the telemarketer.

3.2 Analysis of system for telemarketer

3.2.1 From the concept of registration of telemarketers, it was envisaged that RTMs will directly deal with the Content Providers (CPs) and traffic directly picked from CPs will be delivered directly to OAPs. RTMs are supposed to scrub the list before making over traffic to OAP. Involvement of other RTMs in tandem between CP and AP was not expected. RTMs were also expected to maintain the database of headers assigned to CPs with necessary details about a person or entity who is assigned a header. To trace or contact CP whenever needed RTM connected to AP was expected to directly find out CP in a short interval and provide necessary information or documents from concerned CP e.g. confirmation of consent for opt-in given by a customer.

3.2.2 However, it is noticed that in many cases, there are more than one RTMs involved in the delivery channel i.e. there is a chain of entities involved in between CPs and APs. Intermediate entities may be other RTMs or aggregators just playing a role of aggregating traffic from various CPs. In such cases, there may be many RTMs who have not have taken any telecom resources from APs. Such RTMs may not be using services of NCPR e.g. downloading data periodically. Such RTMs may be just picking traffic from CPs and transferring it to other RTMs connected to APs. They may not be carrying out activities like scrubbing.

3.2.3 The depth of chain of RTMs or aggregators in tandem may vary and may be much deeper in some of the cases e.g. more than 4-5 entities in the chain. RTMs sitting behind in the chain may be dealing in telemarketing business from various CPs on basis of registration as a telemarketer with TRAI. They may be having advantage of not burdened with

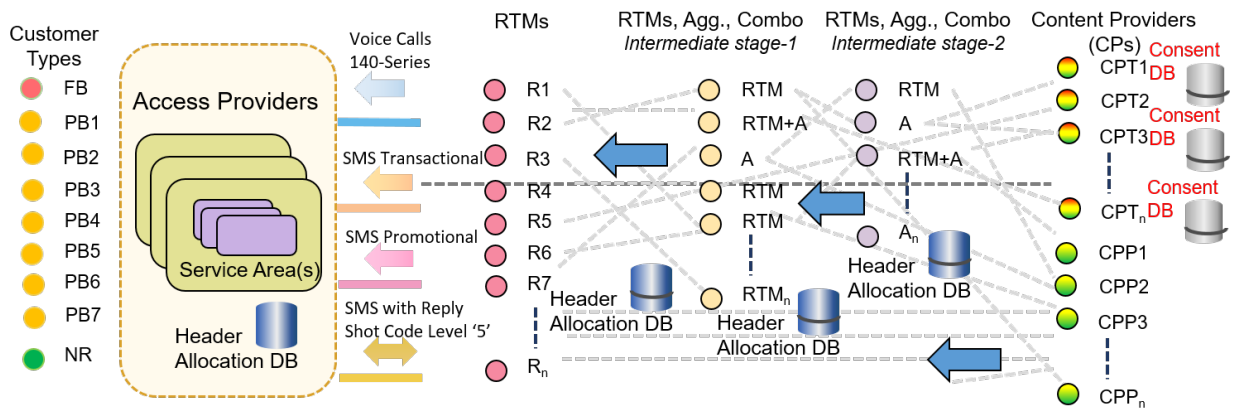
requirements of depositing Security deposits with the access providers or need to have any IT infrastructure and manpower to comply with regulations like scrubbing. Traffic from such RTMs will pass through another RTM which is directly connected to AP and regulatory related requirements are met by that RTM. Such type of RTMs operating from behind may be many in numbers and may be serving niche market areas.

3.2.4 In chain of RTMs in tandem, RTM directly connected to AP, in addition to RTM functions is also doing a role of an aggregator in effect. However, from access provider perspective, last RTM may only be seen and may not be aware about other RTMs sitting behind. From regulatory perspective, RTM directly connected to AP may only be visible and all actions in case of any non-compliance may be taken against first RTM interfacing to OAP. Such RTMs may be burdened with additional responsibility of complying to regulatory requirements for traffic received from other RTMs but they may also be benefited by dealing with large volume of traffic. Large volume of traffic may give commercial advantage to RTM carrying traffic from other RTMs and may also give opportunity to optimally utilize the IT infrastructure which was deployed for its own purpose, may be used for purpose of other RTMs as well. For discussion purposes, such RTMs may be called as RTM+A i.e. RTM with additional role of Aggregator.

3.2.5 In the chain, there are other types of players as well, who are neither RTM nor CP, they are playing a role of aggregation only. Such players might not be registered with TRAI as a Telemarketer but involved in picking traffic from CPs and handing it over to RTMs. Such players may be providing platform for providing interface for a number of content providers to RTMs. They may be involved in selecting RTM(s) on behalf of CPs, playing role in the assignment of header to CPs, maintaining the header assignment database and various other functionality. From perspective of a CP, these players may be a virtual telemarketer entity. Such players and RTMs in the mid of chain may not be willing to share details of persons or entities with other entities in the chain for protecting their market. Such players are not presently defined as a category in the regulation, however such players may be referred as Aggregator only (A) for discussion purposes. These aggregators may be required to be identified and reached for regulatory perspective e.g. to retrieve header assignment details, to get specific details about consent for opt-in from concerned CP.

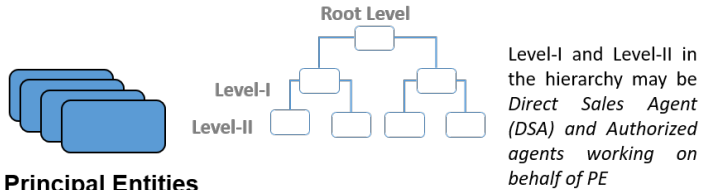
3.2.6 From regulatory perspective, involvement of chain of entities to deliver content from CP to AP, poses a difficulty about retrieving header assignments or consent related details as it becomes a multi-stage process. Consent obtained by the transactional message sending entity (TMSE) are not immediately available with RTM or an aggregator involved in between. Similarly, header related details including person or entity originating content may

Chain of Entities Involved in Telemarketing



Note: Some of the Header Allocation DB may have only the list of headers and there may not be all the details about the header e.g. name and contact details of content provider to whom particular header is assigned.

Multi-level Hierarchy



Principal Entities

A: Aggregator for traffic from RTMs or Content Providers	AP: Access Provider	Consent DB: Database for maintaining records of opt-ins from customers	CP: Content Provider	CPT: Content Provider Transactional
CPP: Content Provider Promotional	CT: Customer Type categorized on the status of registration on NCPR	FB: Customers registered as Fully Blocked on NCPR	Header Allocation DB: Database for maintaining records of Headers assigned and Person or entity	LSA: License Service Area
NR: Not Registered i.e. customers not registered any preferences on NCPR	PBn: Customers registered as Partially Blocked for Category n (n-1 to7)	PE: Principal Entities i.e. Principals on whose behalf content is being sent	RTM: Registered Telemarketer	RTM+A: Registered Telemarketer who is Aggregator as well
TAP: Terminating Access Provider	TMSE: Transactional Message Sending Entity	UTM: Un-registered Telemarketer		

Figure 3.1: Chain of Entities Involved

not be available with a RTM directly connected to OAP or RTM or an aggregator involved in the intermediate stages. These details may be available only with the RTM or an aggregator which is a first interface with the concerned CP i.e. just next to CP in a chain of entities.

3.2.7 Regulations bound RTMs and TMSEs to perform certain activities and comply with certain regulatory requirements through the standard agreements between OAPs and RTMs or TMSEs. These standard agreements are prescribed in the schedules of regulations. However, these standard agreements becomes applicable only for those RTMs or TMSEs who have taken telecom resources from the OAP as these agreements are entered into at the time of taking telecom resources from the OAP.

3.2.8 Unregistered intermediaries and operating without entering into a standard agreement may result into a regulatory enforcement challenge. For example, taking action against these intermediaries in case, they are indulged in any unauthorized or illegal activity. Registration of intermediaries and entering into standard agreements among entities involved in the chain may be needed for division of role and responsibilities among entities. Absence of this poses a challenge to take appropriate action in some of the cases e.g. in case of fraudster types of messages, RTMs or aggregators may argue that content is not originated by him and they are not in a position to examine the nature and characteristics of the content. Similar types of arguments may also be given in case of misuse of transactional pipe for promotional purposes on the grounds that RTMs are performing scrubbing but not screening the content. With large volume of commercial communication traffic screening may be really difficult to be carried out at subsequent stages after origination of content from the source as there are no reference templates for different types of content which may helpful for determination of deviation.

3.2.9 In present system of registration of telemarketers, trace-ability of person or entity registered as a telemarketer is dependent upon the documents submitted at the time of initial registration. There is no provision for verification at periodic intervals. To ensure trace-ability of the telemarketer, there may be a need of robust verification mechanism for submitted documents. This may be helpful to identify and reach to a particular person or entity registered as RTM in case, some illegal or unauthorized activity is allegedly carried out by that RTM. Proper identification may also be required to relate individuals or legal entities who are getting registered with different access providers or in different License Service Areas. It may be helpful for enforcement of regulation for the blacklisted cases i.e. not allocating telecom resources to such individual or legal entity.

3.2.10 With more number of dimensions in the preference categories e.g. sub-categories, time-slot and registration of headers with intended purposes, changes in the scrubbing solution may be required. Scrubbing may required to be enhanced from just scrubbing against list of telephone numbers listed in NCPR with the target database available with the RTMs. And frequent changes may be there in the status if, timeline for preference registration is reduced from the current timeline of seven days. Scrubbing may also be required to be applied in conjunction with set of headers and associated data with the headers e.g. intended purposes. Scrubbing as a Service may handle these complexity in better and easier way. There may be a requirement to scrub the content providers against the purpose of header for which it is intended to be used.

3.2.11 Another issue is related to leakage of NCPR data available with RTMs. It has come to notice that there are websites providing services to scrub for public. It may also happen that the data downloaded by RTMs from the NCPR database may land into the hands of unscrupulous elements, if RTMs are either not protecting the data properly or they are in the nexus with UTMs for carrying out unauthorized activities. UTMs may be exploit this data for making calls or sending messages to customers who are not registered and these UTMs may not get noticed by regulator as complaint from such customers is not entertained by the access providers. UTMs which have taken mobile connections on fake documents, may exploit this data for calling or sending messages to the customers registered on NCPR and may not be contacted by RTMs or TMSEs. Even if such UTMs are caught on the basis of complaints received from the customers, by the time they are disconnected they might have succeeded in their intended purposes. Such UTMs gets re-appearing after getting new mobile connections against new fake documents. In case, NCPR data is not available with UTMs then there is high probability to catch hold of them as they can not restrict their target list within unregistered numbers. There may be a need to have strong provisions for the protection of NCPR data and mitigating problem of UTM.

3.3 Analysis of system for TMSEs

3.3.1 In addition to RTMs, regulation has provisions for Transactional Message Sending Entities (TMSEs).The TMSEs can have direct connectivity with access providers and send transactional messages in accordance to the provisions in the regulations to the customers. TMSEs can also send transactional messages through RTMs. Exemptions provided to certain categories of organizations or purposes in some of other countries are detailed in Annexure-II. As per present regulations, TMSEs may communicate in following cases:

- Information sent to a customer by TSP or Bank or financial institution or insurance

company or credit card company or depositories registered with SEBI or DTH Operators pertaining to the account of its customer.

- Information given by Airlines or Railways or its authorised agencies to its passengers regarding travel schedules, ticket booking and reservation.
- Information sent by e-commerce agencies in response to e-commerce transactions made by their customers.
- Information sent by a company or a firm or depository participant, registered with SEBI or IRDA or Association of Mutual Funds in India or National Commodity & Derivative Exchange Ltd. Or Multi Commodity Exchange of India Ltd. to its clients pertaining to the account of the client;
- Information sent by a registered company to its employees or agents or customers pertaining to goods or services provided by it;
- Information sent by a registered company or charitable trust or society or telecom service provider, pertaining to its services or activities to the telecom subscriber in response to a verifiable request of such subscriber;

3.3.2 In above para, entities which comes under TMSE are clearly specified, to whom they can send the messages is also obvious and restrictions on scenarios when transactional messages can be sent are also specified. TMSEs may be well known entities or they may be less known or they may even entities which are almost unknown as list of exemption include large range of entities by including registered companies, e-commerce agencies, authorized agencies, charitable trust, society etc. There may be a very large number of entities which can be TMSEs and may be known for regulatory purposes only in the cases when they take telecom resources from the Access Provider otherwise not. Every content provider is assigned a header but there are several lakhs of such headers and mapping of header to the content provider is not available at a centralized place. There is no specific provision for verification of documents and details about the content provider assigned a header. In case, TMSEs are sending traffic through other RTMs or Aggregators then for all purposes, they are to be traced through a series of entities in the chain. In the ecosystem having a large number of TMSEs with multiple layers of entities and having many-to-many connectivity matrix there may be a labyrinth of paths to be crossed to reach to the concerned TMSE. There may be a need to put system in place to identify them and contact them whenever they are required to be traced or contacted.

3.3.3 Conditions have been defined for TMSEs to whom they can send messages e.g. to its clients, to its passengers, to a customer, to its employees or agents etc. In some cases like Banks, Credit Card companies, Insurance companies, telecom service providers, DTH operators etc. client or customers may be for a longer period while in some other cases like Airlines, Railways, Registered companies, e-commerce etc. it may happen that relationship of client or customer or passenger is for a very short period. It may also happen that passengers travelling frequently or purchasing goods or services regularly from certain entities may have an account for log-in and conducting transactions quickly without the need of providing same details again and again. It is obvious from this that in certain cases client or customer data may be available for a longer period while in some other cases, it may be very dynamic and short-lived. One company may be dealing in number of products or product ranges and similarly service and bouquet of services. There may be cases, when a customer has created an account with a company but no specific details for the products or services have been mentioned. Such companies might be indulged in sending messages to its clients or customers having account with them. These companies are also indulged in sending promotional messages as a part of transactional messages. Entities involved at subsequent stages may face difficulty in identifying such mixed messages without pre-defined templates for such transactional messages. There may be a need to have a system in place to verify from client database of TMSE to check compliance of the regulatory requirements.

3.3.4 It is noticed that many TMSEs are taking consent from the customer at the time of purchasing goods or services for sending messages or calling to them for commercial purposes. Consents are being taken in various forms e.g. punching telephone number in the computerized at the time of making payment or while taking feedback about the goods or services. There is no robust mechanism adopted by most of the TMSEs to verify the ownership of number provided by the client. Customers are also not aware about the purpose for which number is being shared. Consent are also being taken through web portal or Mobile Apps. Verification of consent at a later stage, poses first challenge to retrieve the information from TMSE database, secondly authenticity of consent. It is also difficult to confirm the scope of consent as it may be including the permission to send promotional offers. All the data related to consent is in the possession of TMSE and there is no way to check it independently. There may be a need to specify standard template for taking consent for commercial communication purposes. There may also be a need to have system in place to record the consent in an verifiable manner which is immutable and non-repudiable. There is also a need to renew consent on regular basis in a verifiable manner and also to have an option to revoke the consent any time by the customer irrespective of its previous permissions. There may be a system in place to keep records of renewal or revoking in a manner verifiable

independently.

3.3.5 Another challenge to verify the messages sent by TMSE is regarding the purpose or activity for which it is being sent. There may be multiple modes of communication between customer and TMSE e.g. query about product or services is raised by a customer through website and reply to query, at a later stage, is being sent through SMS. Reply may be for same or similar products or services. If a customer is in fully blocked state or in a partially blocked category not related to the category for which query is raised, then sending message to the customer may be considered as not in compliance to the regulation while customer was keen to get reply for that query. Sometimes such consents are being taken by TMSE during a voice conversation or through web portal and such consents are quite broad in their scope. In such cases, customer may be getting messages from TMSE on variety of products or services in which he may not be interested in. Mobile Apps facilitating to purchase a range of products or services may put consent as part of terms and conditions at the time of installation of such apps and customer may not be aware of. Verifying these modes of consent is very challenging if there is no system available to record consent and make it available to an independent agency for verification purposes at a later stage.

3.3.6 As of now, several lakhs headers have been assigned to different content providers for the purpose of transactional messages. Customers have no choice to stop transactional messages. Initially, concept of transactional message was started to facilitate certain important and sensitive communication to customer even when he has opted for fully blocked category so as to ensure that such messages reach to him. In present scenario, the very purpose of transactional messages have been defeated. The important issue is how to segregate the transactional message of critical nature with others and create a separate category for less important other messages which can be stopped under the option of customer. In view of this, there are two types of requirements. First, how to reduce the number of transactional messages and second to have system for taking consent, which are verifiable in a non-repudiable manner and keeping records which are immutable. Having option of unsubscribing at any stage may also be desirable irrespective of previous consent of the customer. This option may be required even for customers who are not registered preferences with NCPR for any type of blocking. At present, TMSEs are not registered with NTR and for checking regulatory compliance there may be need to get them registered ensuring the visibility of operational TMSEs. Registration of TMSEs may be required irrespective of allocation of telecom resources to them.

3.3.7 It is observed that some of TMSEs delegates their telemarketing activity to number of agents known as Direct Sales Agents (DSAs). This may be further delegated to entity

at lower level and so on. This becomes a multi-level hierarchy of agents. These agents may be distributed across geographical regions and may also be dealing in different types of products or services. Main entity on whose behalf commercial communications are being done are known as Principals or Principal Entities (PEs). In figure for Chain of Entities in earlier Para, shows this hierarchy. PEs are at root level of hierarchy while agents may be at different levels. At present, header is assigned to individual entity and they do not have any relation with the headers assigned to other entities belonging to same PE.

3.3.8 In thirteenth amendment to the regulation, it was also noticed that a large number of complaints received from consumers pertain to calls or messages originated by or on behalf of banks, insurance companies, builders etc. who are promoting their business by engaging unregistered telemarketers in total disregard of the regulations. These organizations, being the principal are equally responsible for the non-compliance of the regulations and directions issued by the Authority to address the problem of UCC. It is the responsibility of these organizations (the principals) to ensure that the telemarketer engaged by them (the agent) for promoting their business either directly or through an intermediary follows all rules and regulations and if such organization (the agent) fails in this responsibility, they (the principals) are to be held responsible for the acts and omissions of their agents. In order to make these entities accountable, it was decided to amend the regulations to provide for disconnection of all telecom resources of such organizations if they are found to be engaged in telemarketing through unregistered telemarketers. View was that disconnection of the principal entity's telecom resources will act as a deterrent and inculcate a greater sense of responsibility in these organizations.

3.3.9 Even today situation has not changed much in this regard and similar practices of using UTM routes for making commercial communications are continuing. It has been seen that for contacting wide variety and number of customers for sale of products and services, agents are exploring ways to establish dialogue with the customer to explain features of product or service in detail. It tempts some of the sales agents to take unauthorized route to contact the targeted customers. For this, they may be using 10-digit normal subscriber number either themselves or may ask somebody else to work on their behalf for contacting customers to meet their sales and marketing target. Whenever persons working on behalf of authorized agents get a lead in a case, then they may pass it to an authorized agent. If complaints against UTMs are analyzed for finding out the concerned PE indulged in such activities and reported to them for taking action against them then PEs usually disown the responsibilities and argue that these activity is carried out without their authorization and they are not aware about the persons who are indulged in these activities. PEs usually

file a complaint with the police to take action against alleged UTMs working in their name without any authorization from them. Principal Entities may be required to have tighter control on their DSAs or authorized agents working on their behalf. There may be need to develop a mechanism which helps to identify DSAs or authorized agents of PEs by customer at the time of receiving commercial communication. There is also need to have functionality in such system to provide capability of PEs to manage their DSAs or authorized agents.

3.3.10 It is observed that there may be a requirement of TMSE to call customer for transactional purposes in certain cases e.g. alert about high transactional value, OTP through voice call, voice signature for transaction etc.. At present, there is no provision for TMSEs to make transactional voice calls. In practice, many TMSEs are contacting the customer through a normal 10 digit telephone number. Customer is not sure, whether he is being contacted by an authorized person or agency or organization. Some social engineering attacks are being done by unscrupulous elements and they personalize communication with similar type of introduction and questions as of a TMSE. In absence of robust mechanism to identify and authenticate the communication, unscrupulous elements may be able to fetching details from the customer in an unauthorized manner.

3.4 Analysis of system for content providers

3.4.1 At present, Content providers are identified on the basis of header assigned to them. Headers to CP are assigned by a RTM. RTM communicates headers to originating access provider through which traffic is to be handed over for delivery. However, details of headers may only be list of headers and not other details like name and contact details of persons of CP to whom a particular header is assigned. Specific purpose for which header is assigned may also not be known. There is no central repository of headers assigned to the CPs to ensure uniqueness of headers or facility for online access to details about headers and CPs. Uniqueness is maintained within chain of entities through which content has to pass from CP to OAP. Entities may require to mark headers as white labelled in their system for identification and authorization purposes. It may happen that same header is assigned by another RTM in different chain of the ecosystem. However, two character code corresponding to an OAP is prefixed and header presented to a customer is unique. However, last six characters which are associated with the CP may not necessarily be unique.

3.4.2 CPs may have connectivity with multiple entities through completely different chain of entities. This may also be required to build redundancy, for example in case of financial transaction, alert message may be required to be delivered to customer with high reliability.

In such cases, same CP may have multiple headers. Differences in multiple headers may be as little as change in prefix corresponding to a AP or Service Area or it may be completely different header.

3.4.3 Identifying CP on the basis of text string of header presented to a customer may sometimes be misleading as it may resemble with well known entity who may not be the actual CP which customer has believed to be. Such misleading due to resemblance of header may be inadvertent or may be deliberate attempt of some unscrupulous elements. Sometimes it may not be possible for CP to get header which reflects its usually known name as preferred header string might already be assigned to somebody else. There may be cases of squatting on headers resembling to names of well known entities. Such situation of header assignments and customer interpretation of CP through header strings presented to him may be exploited by some unscrupulous elements. SEBI has raised similar issues indicating that some of CPs are using header names which resembles with well known brokers registered with SEBI to make believe customers that message is from well known entity. RBI has also raised concerns about misuse of same or similar headers to mislead the customers. There may be a need to have central repository of header assigned to CPs. This may help to avoid assignments of same or similar headers to different entities. Guidelines to avoid headers matching in proximity to well known entities may also be required. There may also be requirement to assign block of headers to Principal entities for its DSAs or authorized agents.

3.4.4 It is also observed that there is no track of its regular usage by the assignee of header. It may happen that many headers which were assigned to CP may not be in use today. There is possibility of misuse of headers by other parties as it may be white listed by many entities in the chain as they may not be aware about the use of header by other unauthorized CP. There may be reassignment of header from one CP to another CP for example, headers used for a campaign during festive days may be short lived. Same header may be reassigned or recycled for different short lived campaigns belonging to different CPs. There may be a requirement to manage life cycle of header assignments. It may helpful in avoiding chances of misuse of header assignments.

3.4.5 It has come to notice that content delivered to a customer may be required to be authenticated. For example, if doubt arises about a content and customer wants to verify whether content has originated by an entity he is made to believe from the header or content details then there should be some mechanism to authenticate this. For example, if a message is received by a customer related to accommodation requirement for installation of a mobile tower and one wants to confirm from Infrastructure provider licensee holders whether it is a genuine message or a fraudulent message then at present there is no mechanism available

to verify. Availability of such mechanism may immediately bring to the notice of concerned organizations about the suspected activity.

3.4.6 It is felt that there is a need to demarcate the role and responsibilities for content provider through a standard agreement which may pro-actively mitigate misuse of transactional headers for promotional purposes. Identification and registration with mechanism for content authentication may be helpful for avoiding to fall prey to fraudulent promotional offers.

3.5 Options to make system more effective and efficient

3.5.1 National Telemarketers Register (NTR)

i. For addressing the issue of trace-ability of intermediate entities in the chain including content providers, one of the option may be to make the requirement for registration of all such entities. There may be a need to specify various documents which may be required to be produced by such entities at the time of registration. There may also be need to have robust mechanism to check the authenticity of documents being submitted. Once entity is identified with proper registration and verification process then it may be required to enter into the agreements with other relevant entities. Agreements may be based upon reference templates specified from regulatory perspective. Robust mechanism of verification and authentication may be required for RTMs as well to avoid possibility of reappearance of blacklisted RTMs in some different name and form. It may require introduction of measures like eKYC, online or digital payment channels, additional documents, online verification of documents, verification of email and phone number through one time password (OTP) etc. There may also be need to verify mobile number and email on regular intervals.

ii. Present National Telecom Register (NTR) may be required to be upgraded or revamped. New NTR system may need to handle registration of all types of entities and during complete life cycle. Such system may provide capability to verify the activities, records without depending upon entities who are alleged to be involved in the malpractices.

iii. Given the numbers of such entities, there may be a need to have new NTR system with digital infrastructure and automated process. This system may be required to deal with complex and quite big matrix of agreements among different entities. However, with the evolution in the Information Technology (IT) arena, and availability of latest solutions, it

may be possible to digitize and automate the process and provide platform to participate all entities on a online system with real or near real time executions of the process. For making scalable system, option may be to move from traditional physical servers to cloud based systems. It may provide capability to deal with high volume of transactions. There is a need to explore options for systems which can create records of activities in an immutable and non-repudiable manner. Depending upon the suitable solutions, Establishment of scalable system with capability to control and manage the process may likely bring good insight into the system and grip over operation of complete ecosystem of telemarketing activities.

iv. New NTR system may either be established, operated and maintained by TRAI or an agency authorized by it or it may be outsourced. Another option may be stipulating key requirements of desired system and allow independent agencies to develop such systems and solutions. Rights to establish and operate such systems may not be on exclusive basis and there may be multiple agencies. However, there may be requirement to synchronize the databases of multiple systems or to have single logical view for users of the system. Terms and conditions for exit from running such systems by agency and complying to regulatory requirements may also be required. There may also be an option to establish and operate such systems by consortium of relevant stakeholders.

v. There may be option to have phase wise implementation of the system and options to define levels for participation in the system. Some sectors e.g. Finance related markets may be more sensitive and particular about the requirements to be met while it may not that serious for other sectors. Phase-I of implementation may not require participation of everybody for all purposes. In some cases, level of participation may be voluntary. In subsequent phases, gradually participants and level of participation may be increased.

vi. Having such system having on board all the entities in the ecosystem may bring lot of efficiency in all aspects. Such a system provide capabilities to enter into the agreements and revoke these agreements as and when required by the authorized entities in smarter ways. In addition to insight into the system, it may bring control and management of life cycle of entities and process. It may reduce time to become part of the system as well as remove the entities from the system whenever they are not complying to the regulatory requirements.

3.5.2 Customer Consent Recording System

i. To address the issue of TMSEs sending transactional messages to their clients in the name of taken a consent from the customer, there may be a need to have robust mechanism for recording consents of customers for opt-in. Recording of consent need to be recorded in a

manner which is immutable and non-repudiable. There is also need to have provision for customer to withdraw or revoke the consent any time. There may be need to have provision for modifying the scope of the consent by the customer as well. At present, such consents taken by TMSEs may only be available with them. This may require to stipulate detail procedure for taking consent. It may also include reference templates for taking consent.

ii. For the purpose of robust mechanism to record the consent and online accessibility to consents for verification purposes there may be need to develop digital and automated process. One option may be that TMSE may develop their own systems which are robust systems for verification and authentication purposes. In this case, TMSE may continue to keep the consent related documents or database with themselves. However, TMSE may need to allow reach and access to these documents using online and secure system. However, TMSEs are very large in numbers and may not be operational 24x7 for retrieving the requisite information. Moreover, they may not be willing to provide access to external agencies for security related aspects.

iii. Alternatively, build a centralized system for consent related documents. Authentication of customer may be carried out by sending One Time Password (OTP) from a centralized system which may be used to record the event of consent. This process may be good to record that transaction has happened but may not be good enough to ensure the scope of consent. It may need to keep consolidated documents from all TMSEs, which may be impractical to implement.

iv. Another option may be to record only relevant part of the consent process in a verifiable and authenticated manner. It may be based upon interactions with TMSE systems and also have process to record scope of consent. For example, reference templates for taking consent in different scenarios are pre-defined and registered with the system. The consent templates may be purpose specific or entity specific or combination of both. Consent template, dynamic content, parties involved, time and day of consent etc. may produce a hash code which may be used for verification and authentication at a later stage. If such systems are working in a distributed manner then they may be scaled to very high capacity and may be optimized for the requirements. These systems may require to keep confidentiality of client database of TMSEs.

v. Consent recording system need to be integrated with multiple modes of taking consents e.g. through web portals of companies, Mobile Apps, during a conversation with call centre executive etc. System need to have provision for registration of consent template including the scope of consent. provision for revoking consent or modifying the scope of consent by

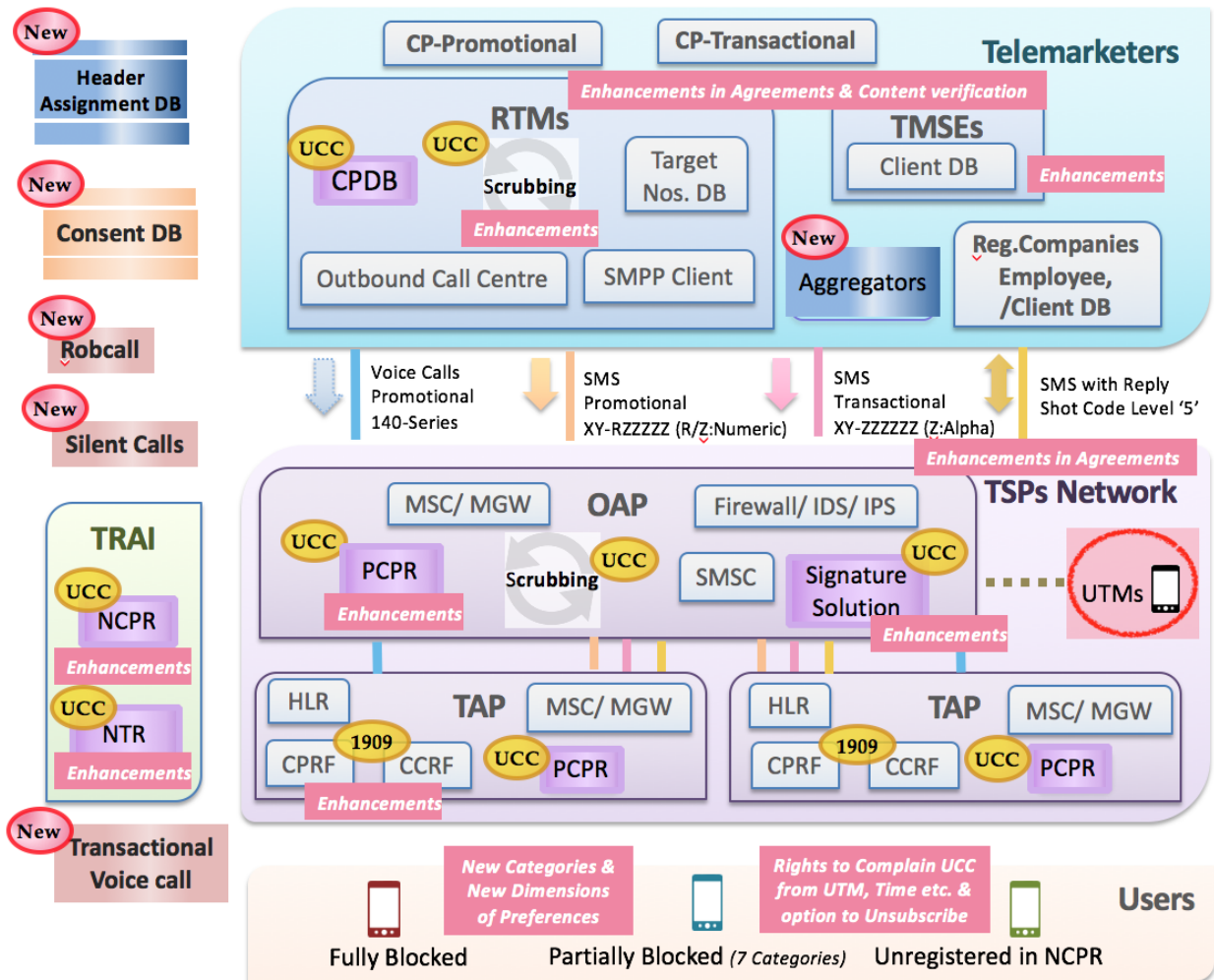


Figure 3.2: UCC Ecosystem(New Entities)

the customer irrespective of previous status. Process of revoking or modification of consent may require reference to a previous consent, which may be required to be developed in a user friendly manner so that one can select from the options of probable consents given by the customer. Such solutions may be developed by industry initiatives and with involvement of relevant stakeholders.

vi. Recording, withdrawal and modification of consent may be applicable for all types of customers i.e. fully blocked, partially blocked or not registered with NCPR.

3.5.3 Content Template Registration and Verification System

i. For addressing the issue of some of TMSEs misusing transactional pipe for sending promotional messages there may be need to screen the content sent by TMSE. RTMs may need to have system which can screen content for a large volume of traffic passing through it.

To read and validate individual SMS may be a challenging task for any entity in the chain. Primary responsibility may be of content provider and in case of non-compliance, CP may be held responsible.

ii. Another option may be to develop mechanism which can ensure that content is meeting regulatory requirements. One option may be to have reference content templates for specific purposes on similar lines as discussed for consent templates. There may be mechanism to generate content identity and hash codes using necessary parameters and content which can be applicable for 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 TMSEs.

iii. There may be mechanism to authenticate the content by the customer by submitting content id and hash codes to well known entity which customer may be aware of. For example, if investment tip is received from a CP and customer has a doubt whether it is originated from same entity which customer is believing then he may have to submit content id or hash code either to SEBI or SEBI registered entity for authentication purposes or to an independent agency responsible to keep records of reference templates or to CP. For such mechanisms the role and responsibilities of CP may include content template registration for different purposes consisting of content id generation, associated list of customers with hash codes of content etc while for intermediaries the roles may include screening of content on basis of content ids and corresponding recording of hash codes.

3.5.4 NCPR Data Protection

i. To protect NCPR data from reaching to unscrupulous elements, one way may be to set provisions and guidelines to RTMs for maintaining data in a secure manner. But it may not be helpful if some RTMs are deliberately indulged in such unauthorized activities. Another option may be to introduce scrubbing as a service and thus not allowing anyone to download data of registered subscribers who do not wish to get telemarketing calls. In this case, RTMs may be uploading list of target numbers and may get scrubbed list as a result of it.

ii. Another leakage point may be unscrupulous elements having automated system to query NCPR portal for a series of individual numbers and generates parallel database. They may also be generating on basis of demand and fetch the details specific to numbers. One option may be to make the requirement to authenticate at the time of query to NCPR portal. One of option to authentication may be done using through OTP. Protection of NCPR data,

ask access providers to entertain complaints also from customers who are not registered on NCPR

3.5.5 PE DSA Management System

i. Issue related for having tighter control of Principal Entities (PEs) over their DSAs and authorized entities may require a systematic approach. One of the first requirement may be to bring all DSAs and authorized under one umbrella of concerned PE so that they can be identified as a single logical entity. For this purpose, DSAs and authorized agents of Principal Entities (PEs) may need assignment of block of headers instead of uncorrelated headers.

ii. Option may be to assign a shorter length headers to PE for root level entity. PEs may further assign remaining characters or digits to its lower level entities. To give flexibility to PEs, they may require interface to a new NTR system to manage their DSAs and authorized agents themselves. Functionality of such a system may include option for assignments, de-assignments, managing complete life cycle of headers etc.

iii. With this PEs may be having better control and management over their DSAs and authorized agents e.g. putting header into a suspend mode, active mode, de-active mode etc. It may help PEs to have better control over commercial communications originated by their DSAs or authorized agent. From regulatory perspective, it may apply regulatory requirements to PE instead of its delegated entities. However, system may have records of all activities of PEs and verifiable in an independent manner.

iv. In conjunction with granular choices for preferences and options to set prefer days and time, PEs may be able to contact interested parties in accordance to the preferences of the customers. Capabilities to take consent in verifiable and authenticated manner and keeping client database in confidential and secure manner may encourage to all telemarketers to take permissible route. With better control and management of PEs over its agents may likely help to eliminate problem of UTM on behalf of PEs. If PEs are found even after implementation of such flexible and facilitating system then there may be requirement to impose severe penalty provisions on defaulter PEs.

3.5.6 Format and Structure of SMS Header and voice calls

i. With increase number of choices in the preferences discussed earlier, associating purpose with the header etc. there may be a difficulty in the scrubbing process on the basis of

present header format and structure. Another requirement to change of format may come from assignment of block of headers to PEs on chargeable basis. Requirement of leaving some of headers or reserving them to ensure that they are not having proximity match with headers of well known entities may eat out Name or Numbering space of Headers. One option may be to increase the length of headers but there may be technical limit of maximum number of characters which may be used in SMS headers. Another option may be to include additional characters required for identification of categories as part of content. One more option may be doing scrubbing on basis of hash codes instead of headers. It may require changes in the scrubbing process and process for generation of hash codes by relevant entities.

ii. There may be a possibility to have complete trace of the route e.g. signatures of all entities through which content has passed. At present prefixes related to OAP are part of headers, in case additional characters are introduced as a part of content then more details may be available about the route a content has taken. Alternatively, there may be argument to not to have such functionality as there may be a mechanism to authenticate the content. But in case, content is not authenticated then it may be required to identify the culprit.

iii. For facilitating TMSEs to make voice calls for well justified reasons and legitimate purposes e.g. alerting and verification by banks in case high value transaction has happened, there may be need to have separate series for these types of calls on similar lines as in case of promotional voice calls. Presenting same number or a number from similar sub-series assigned to a particular PE may help to customer to identify the PE. With operation of DSAs and authorized entities of PEs from various locations and also using mobiles solutions which require to call from fixed locations may not work. Intelligent Network (IN) based solution or IP Multi-Media Sub-system (IMS) based solution may probably help to establish a system which presents calling line identity to a customer reflecting identity of a PE.

In view of above analysis and options which may be used to make registration of system of telemarketers more efficient and effective, and introducing new entities and process, suggestions and inputs of stakeholders are sought on following

Q. 8. For robust verification and authentication of telemarketer getting registered, what changes in the process of registration, may be introduced? Please give your suggestions with reasons.

Q. 9. Should registration of other entities such as content providers, TMSEs, Principal Entities, or any other intermediaries be initiated to bring more effectiveness? Whether standard agreements can be specified for different entities to be entered into for playing any role in the chain? Please give your suggestions

with reasons.

Q. 10. Whether new systems are required be established for the purpose of header registration, execution and management of contract agreements among entities, recording of consent taken by TMSEs, registration of content template and verification of content ? Should these systems be established, operated and maintained by an independent agency or TRAI? Whether agency should operate on exclusive basis ? What specific functions these systems should perform and if any charges for services then what will be the charges and from whom these will be charged? How the client database of TMSEs may be protected? Please give your suggestions with reasons.

Q. 11. Whether implementation of new system should full fledged since beginning or it should be implemented in a phased manner? Whether an option can be given to participate on voluntary basis? Please give your suggestions with reasons.

Q. 12. Whether scrubbing as a service model may be helpful for protection of NCPR data? Whether OTP based authentication for queries made by individuals on NCPR portal may be helpful to protect NCPR data? What other mechanisms may be adopted to protect the data? Please give your suggestions with reasons.

Q. 13. What interface and functionality of NTR system may be made available to Principal entities for managing header assignments of their DSAs and authorized agents? How it may be helpful in providing better control and management of header life cycles assigned to DSAs and authorized entities? Please give your suggestions with reasons.

Q. 14. What changes do you suggest in header format and its structure that may be done to deal with new requirements of preferences, entities, purpose? How principal entities may be assigned blocks of headers and what charges may be applied? What guidelines may be issued and mechanism adopted for avoiding proximity match of headers with well known entities? Please give your suggestions with reasons.

Q. 15. Whether voice calls should be permitted to TMSEs and how these can be identified by the customers? How intelligent network (IN) or IP Multi-media subsystem (IMS) based solutions may be useful for this purpose and what flexibility it may provide to TMSEs in operating it and having control on its authorized entities? Please give your suggestions with reasons.

Q. 16. What steps need to be initiated to restore the sanctity of transactional SMS? What framework need to be prescribed for those transactional SMS which are not critical in nature? Please give your suggestions with reasons?

Chapter 4

UCC Complaint Handling

- Introduces current process of complaints resolution and also explores ways to reduce the time line. Also explains proactive counter actions to identify UCC through the use of signature solutions, Honeypots etc.
- Suggests ways to deal with the false complaints against a person in business/commercial/family relations or due to wrong identification of person.
- Highlights usefulness of TRAI mobile app in complaint filing on different mobile platforms.
- Introduces present provision of Financial Disincentives on Access Providers and explores the need to review it, in view of additional roles and responsibilities assigned to access providers.

4.1 Introduction

4.1.1 In the present framework for making complaints against a UCC, customer can file his complaint through various Customer Complaint Resource Functionality (CCRF) made available by access providers. CCRF includes various modes like customer care number, IVRS, Web portal, email. TRAI has also facilitated customers to file complaint in user friendly manner. However, this mobile app of TRAI is not available on device operating systems.

4.1.2 Complaints are submitted to the Terminating Access Provider (TAP) who is serving the customer. Customer can make complaints within three days from the date of receiving UCC. TAP carries out certain checks like registration status of the complainant, Call Detail

records for verifying that communication has actually taken place. After due verification, which is required to be carried out within 72 hours, if it is found that complaint is valid then it is forwarded to Originating Access Provider (OAP) through NCCPR portal. In case, complaint is found to be invalid then complainant is informed.

4.1.3 OAP regularly downloads all the UCC complaints pertaining to it through NCCPR portal. OAP further examines the complaint with CDR generated on its end and also checks the status of complainant. If it is found that the complaint is valid then it identifies specific details about the defaulting telemarketer or UTM. Valid complaint in case of RTMs may result into issuance of notice, disconnection of telecom resources, deduction of amount from security deposits of telemarketer. In case of UTMs, valid complaint may result into disconnection of telecom resources. For sending UCC, both UTMs and RTMs may be blacklisted for a period of two years and may not get telecom resources from any of the telecom service provider.

4.2 Analysis of UCC complaint handling system

4.2.1 To handle the UCC complaints in a timely manner, time frames for TAP and OAP have been defined. For TAP, time frame for examination and taking action on UCC complaints, within which it has to conclude and take appropriate action is specified as 72 hours. Similarly, time frame for OAP is also 72 hours to examine the complaints and take appropriate action against UTM or RTM as the case may be. It is felt that present time lines for handling UCC complaints is quite long.

4.2.2 At present, access providers are asked to pay by way of financial disincentive if UCC complaints are found to be 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 appropriate 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 doing their due responsibilities. Financial Disincentive of not exceeding Rs. 5000 per UCC complaint is being applied on the basis of total number of UCC complaints for an OAP at all India level in a week. Amount of Financial Disincentive is presently based on slabs of total counts of UCC complaints e.g. between 0-100 it is zero, while between 101-250, it is Rs. 500 per UCC complaint, between 251-500 it is Rs. 1000 per UCC complaint, between 501-1000 it is Rs. 2000 and for greater than 1000, it is Rs. 5000

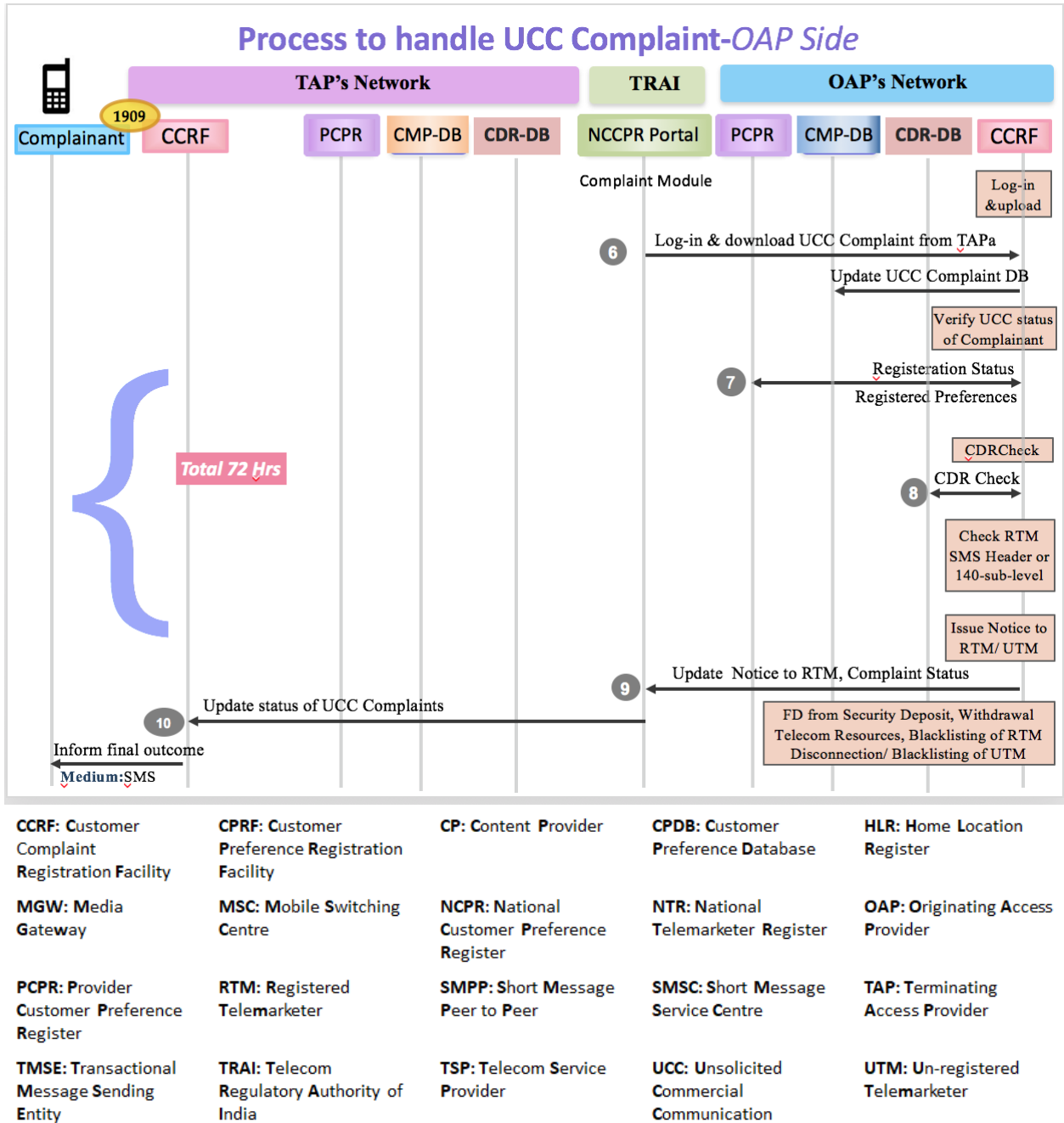


Figure 4.1: UCC Complaint Resolution Process(OAP side)

per UCC complaint.

4.2.3 TSPs have represented, from time to time, against applying financial disincentives on counts of UCC complaints including those UCC complaints which they have examined and took appropriate action against the RTM or UTM within given time frame. They also argue that they do necessary checks and verification at the time of new connection in accordance to the licensing and regulatory requirements. Customer Acquisition Form (CAF) clearly mentions that if subscriber is found to be indulged in sending UCC then action may be taken against them as per the provisions of regulation. Their argument is that for UCC complaints, which are handled within time frame and appropriate action is taken should not be counted for applying financial disincentives as they are not responsible for the unauthorized usage of connection by UTMs.

4.2.4 The present system does not have provision of lodging complaint by the customer who is not registered in NCPR. There are certain circumstances where unregistered customer is required to make complaints like commercial call from UTM, beyond permissible time by RTMs etc. Even such customers may be having concerns due to commercial communications when they are roaming as it may lead to charging of incoming communication. In case, a customer has forwarded a call to another number, then all incoming calls including telemarketing calls will get forwarded and customer may be charged for forwarded calls. RTMs may not be aware whether customer is roaming or has forwarded the call to another number, however mobile app may be helpful to alert the end customer e.g. incoming call is promotional call and roaming charges may apply.

4.2.5 It is found that sometimes UCC complaints are made by the customers who were in business relationship or family or friends of the person against whom complaint is made. For example, one has taken financial loan from an organization and if person from that organization tries to contact him then customer claims this communication to be UCC and complains for taking action. Similarly employee of an organization who is disenfranchised due to some reasons makes an unauthorized call from telephone number belonging to organization to its own number and then claims it to be UCC. It is also found that telecom resources are disconnected of customer on the grounds that UCC was sent from another number belonging to same person while in fact another number was taken using fake documents. Such cases have been verified by DoT offices and it was found that in fact number from which UCC was sent does not belong to the person whose telecom resources have been disconnected.

4.2.6 Access providers are also responsible to deploy signature solution in their networks for taking proactive actions to identify UCC messages being sent by the Unregistered Tele-

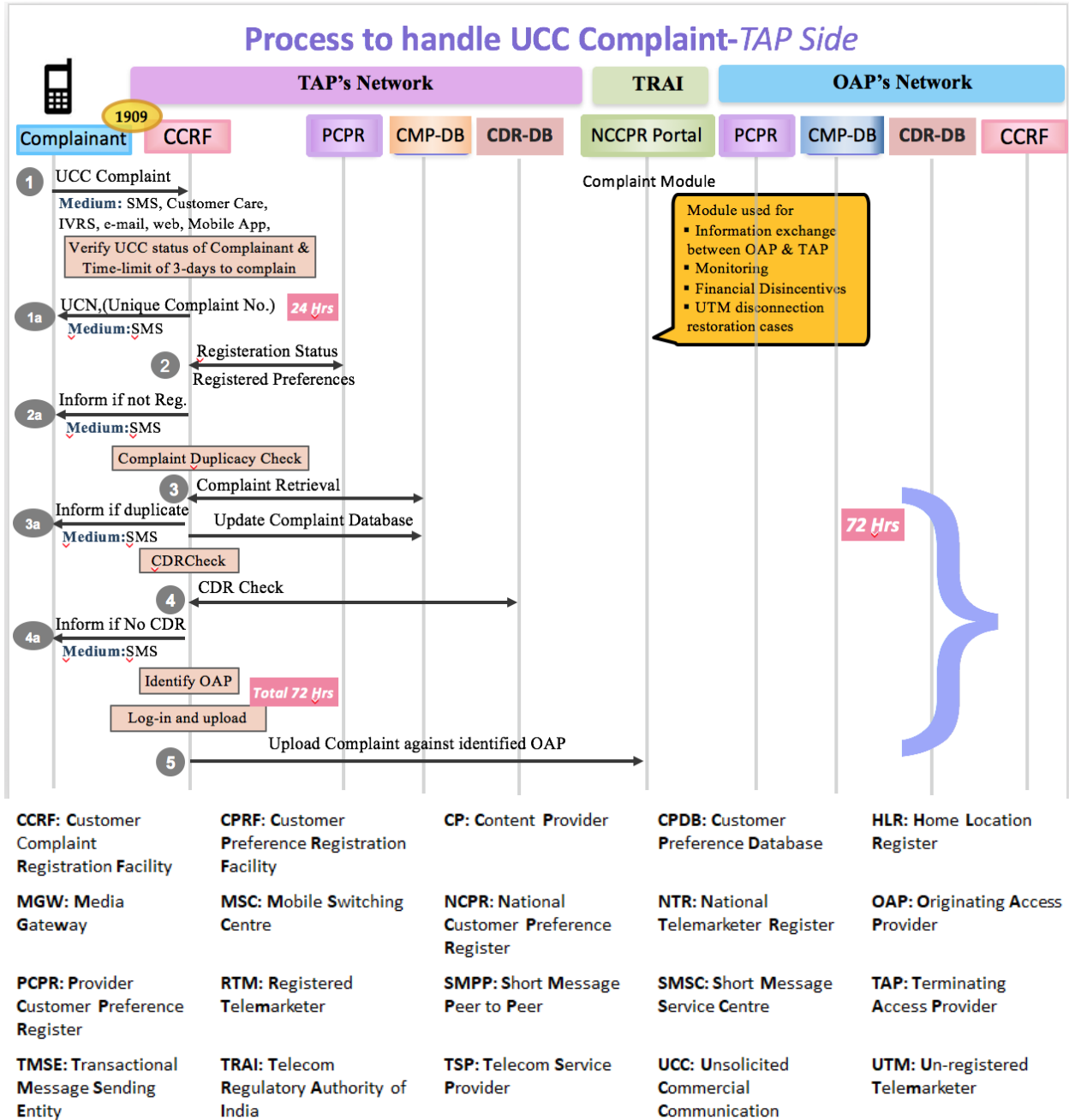


Figure 4.2: UCC Complaint Resolution Process(TAP side)

marketers (UTMs). Signature solutions have dictionary of key words, phrases and have capabilities to do the pattern matching of SMS contents with the key words or phrases available in the dictionary. This process of pattern matching is done on a part of traffic passing through the SMS Centre (SMSC) which is P2P (Person to Person) i.e. coming from 10-digit numbers and only those SMS which are sent by a single number and exceed a prescribed threshold i.e. more than 200 SMS per hour. If such messages are found to be commercial in nature then proactively action is taken against such subscribers for indulging in activity of sending UCC.

4.2.7 It is found that some of the unscrupulous elements, are not getting detected if they are fragmenting traffic originated by them across multiple telephone numbers. These numbers may belong to different access providers. In such cases they are bypassing the criteria set in the signature solutions and not getting detected. In this way UCC messages sent from a particular number is not exceeding the limits set to match the pattern. They are also tweaking the UCC message content e.g. by putting different special characters, by deliberately making spelling mistakes, by using phrases in a different manner than its normal usage. Tweaking of content of messages is done in such a manner that they are able to convey the message to the recipient and same time not getting detected by the Signature Solutions.

4.2.8 In present system action is on individual complaint basis and there is no provision for handling multiple complaints against a single person or an entity. If complaints are consolidated at a centralized place then the complaints pertaining to single person or entity may be analyzed for taking appropriate action immediately.

4.3 Options to make system more efficient

4.3.1 It is felt that present time lines for handling UCC complaints may be reduced as new technological solutions have emerged. Checking and verification of complaint may be expedited with on-line retrieval of data and by doing automatic comparison of claims of complainant with the facts retrieved from the system. Structured and pre-validated inputs from complaints using Mobile Apps and web portals may be helpful to quicken the process and reduce the instances of rejection of complaints. Mobile Apps which function in intelligent and intuitive manner to protect the customer from UCC may require certain permissions from device platforms like contact details, call logs, SMS content, interaction with remote entity, running process in the background etc. If required permissions are not given by the device platforms then customer may be deprived from the rights to protect himself. In view of above, there may be requirement to make mandatory to provide permission by all the

device manufacturers to Mobile App developed by TRAI or agency authorized by it.

4.3.2 In view of representations from access providers and international practices for taking action in case of non-compliance, it may be required to revisit the present provisions for financial disincentives and type of UCC complaints on which it is to be applied to. However, it is felt that if Access Providers are closing UCC complaints in an appropriate manner and not taking appropriate action against the RTMs or UTMs within time frame then there may be a requirement of taking stringent actions against such defaulter access providers. Access providers may also be asked to enhance the capabilities of Signature Solutions already deployed or introducing new entities like honeypots.

4.3.3 Lodging complaint by the customers who are not registered in NCPR may also be permitted in the cases of commercial call from UTM, or from RTM beyond permissible day and time etc.

4.4 Options to make system more effective

4.4.1 Signature solutions

i. Pattern matching in the signature solutions may also be required to be applied on A2P (Application to Person) traffic coming from RTMs or TMSEs. 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 set of headers along with the purpose for which they are assigned. All Access Providers may require to collaborate to evolve signature solutions in a better and faster way. New patterns detected or learned by one Access Provider may be immediately adopted by other Access Providers. criteria of threshold may be applied on logical entity instead of one telephone number and this logical entity may be a set of telephone numbers. Grouping of telephone number purposes may be done on various factors e.g. all mobile numbers which have not changed locations in more than three Cell-Ids of one technology network or ratio of outgoing and incoming messages or calls is very high. Logical entity may also be created with telephone numbers belonging to different access providers and individual access provider may provide total counts of SMS or voice calls originated from sub-set of logical entity. Combining of events captured from sub-sets of logical entities being monitored by different access providers may be shared and criteria may be applied on complete logical entity for determination of subsequent actions. This requires setting up of a framework for

sharing information in an abstracted manner and it also require sharing of rules, criteria and threshold. There may also be need to have signature solutions at RTM end as well to detect misuse of headers by the content providers.

ii. Signature solution is also required to be evolved on continuous basis as unscrupulous elements are regularly changing patterns and trying to bypass the defined key words and phrases by tweaking the content. Signature solutions may also take into account information from other sources like missed call alerts, call forwarding details etc. to analyze the patterns of calls from numbers which are not responded by many customers and numbers used by UTMs to avoid disconnection of original number. ITU Recommendation X.1246 on "Technologies involved in countering voice spam in telecommunication organizations" [8] provides details about using information from various network entities which may be used for identifying spam source. Artificial Intelligence (AI) based solutions and collaborative approach among Access Providers may also help to learn new patterns quickly and apply the pattern on dataset belonging to same entity available with different access providers. It may be helpful to detect and mitigate any misuse by the telemarketers or content providers or TMSEs.

4.4.2 Honeypots

i. Unscrupulous elements some times send messages or make voice calls to series of telephone numbers including numbers which may not be allocated to any subscriber or numbers meant for data connections. If honeypots are created by the Access Providers in their network which are dummy numbers but have characteristics of actual working numbers. Even voicemail box may be allocated to these numbers so that voice calls may be answered by these honeypots. There is likelihood that messages or calls from UTMs may land on honeypots and data collected by honeypots can be used for identifying UTMs and taking appropriate actions. As Honeypot connections may not belong to actual subscribers and also these should not be known in public domain so that unscrupulous elements should be unknown about these numbers.

ii. Numbers identified by honeypots may be input to signature solutions for further analysis of the characteristics of the usage of number. Call Detail Record (CDR) analysis of numbers identified by honey pots and signature solutions may be used to have deeper investigation and find out whether that particular number is being used for commercial communication purposes.

4.4.3 Action on aggregated complaints

i. For taking action immediately against the defaulters against whom a large number of complaints have been reported by different customers, received complaints may be combined and seen together. Aggregation of multiple complaints against such number or such entity may be helpful to detect defaulter at early stage. It may also help to quickly conclude and avoid further misuse. This may require collection of complaints from different access providers at a central place. Alternatively, there may be a possibility to connect different compliant handling systems and pull the information in relevant cases for combining the complaints.

ii. For the purpose of taking action against consolidated complaints, there may be need to collect complaints at a centralized location or have mechanism to pull information from distributed databases located at different locations.

4.5 Cases of false complaints

4.5.1 There is need to have mechanism which avoids or eliminates victimization. Such victimization may also happen even in case of pattern matching with signature solution, if due diligence is not done by the concerned person. At present no common approach among TSPs is there to handle cases identified using signature solutions. In view of this, there may be requirement to develop reputation based analysis of customers so that victimization, if any, may be avoided. Reputation based analysis may take into account various factors like age of subscription, authentication at the time of subscription, address verification method etc. 3GPP Technical Study Report TR 33.937 "Study of Mechanisms for Protection against Unsolicited Communication for IP Multi-Media Sub-system (IMS) (PUCI)" [1] 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). However, similar type of concept may be implementable with signature solutions.

In view of above analysis and options which may be used to make UCC complaint handling process more efficient and effective, and introducing new entities and process, suggestions and inputs of stakeholders are sought on following

Q. 17. To what extent, present gap between time when UCC complaint was made and time when this was resolved can be reduced? What changes do you suggest to automate the process? Please give your suggestions with reasons.

Q. 18. How the medium of Customer Complaint Resource Functionality (CCRF) with pre-validation of data e.g. Mobile App, Web Portal etc. may be helpful

to achieve better success rate in complaint resolution process? Please give your suggestions with reasons.

Q. 19. Whether access providers may be asked to entertain complaints from customers who have not registered with NCPR in certain cases like UCC from UTM, promotional commercial communication beyond specified timings, fraudulent type of messages or calls etc.? What mechanism may be adopted to avoid promotional commercial communication during roaming or call forwarding cases? Please give your suggestions with reasons.

Q. 20. How the mobile App may be developed or enhanced for submitting complaints in an intelligent and intuitive manner? How to ensure that the required permissions from device operating systems or platforms are available to the mobile app to properly function? Please give your suggestions with reasons.

Q. 21. Should the present structure of financial disincentive applicable for access providers be reviewed in case where timely and appropriate action was taken by OAP? What additional measures may be prescribed for Access Providers to mitigate UCC problem? Please give your suggestions with reasons.

Q. 22. Whether strict financial disincentives should be levied for different types of techniques like robocall, auto-dialer calls for UCC? Please give your suggestions with reasons.

Q. 23. What enhancements can be done in signature solutions ? What mechanism has to be established to share information among access providers for continuous evolution of signatures, rules, criteria? Please give your suggestions with reason.

Q. 24. How Artificial Intelligence (AI) can be used to improve performance of signature solution and detect newer UCC messages created by tweaking the content? Please give your suggestions with reasons.

Q. 25. How the honeypots can be helpful to detect and collect evidences for unsolicited communications? Who should deploy such honeypots? Please give your suggestions with reasons.

Q. 26. Should the data from mobile app or from any other source for registering complaints be analyzed at central locations to develop intelligence through crowd sourcing? How actions against such defaulters be expedited? Please give your suggestions with reasons.

Q. 27. How the increased complexity in scrubbing because of introduction of additional categories, sub-categories and dimensions in the preferences may be dealt with? Whether Scrubbing as a Service model may help in simplifying the process for RTMs? What type and size of list and details may be required to be uploaded by RTMs for scrubbing? Whether RTMs may be charged for this service and what charging model may be applicable? Please give your suggestions with reasons.

Q. 28. How the cases of false complaints can be mitigated or eliminated? Whether complaints in cases when complainant is in business or commercial relationship with party against which complaint is being made or in case of family or friends may not be entertained? Whether there should be provision to issue notice before taking action and provision to put connection in suspend mode or to put capping on messages or calls till investigation is completed? Please give your suggestions with reasons.

Q. 29. How the scoring system may be developed for UCC on the basis of various parameters using signature solutions of access providers? What other parameters can be considered to detect, investigate and mitigate the sources of UCC? How different access providers can collaborate? Please give your suggestions with reasons.

Chapter 5

Issues for Consultation

Q.1 To what extent, time required for registration and enforcement can be reduced? For achieving reduced time lines, what changes in processes or in different entities e.g. PCPR, NCPR, CPDB may be required? Will providing scrubbing as a service for RTM reduces time? Please give your suggestions with reasons.

Q.2 How to ensure availability of Mobile Apps for registering preferences and complaints and for de-registration for all types of devices, operating systems and platforms? Whether white label TRAI Mobile App may be bundled along with other Apps or pre-installed with mobile devices for increasing penetration of app? For popularizing this app, what other initiatives can be taken? Please give your suggestions with reasons.

Q.3 In case of Mobile Number Portability (MNP), what process may be defined for retaining the status of customer for preference registration? Please give your suggestions with reasons.

Q.4 How bulk registration may be allowed and what may be the process and documents to register in bulk on behalf of an organization or family? Please give your suggestions with reasons.

Q.5 Is there a need to have more granularity in the choices to actually capture customers interest and additional dimensions of preferences like type of day, media type(s)? What will be impact of additional choices of preferences on various entities like CPRF, PCPR, NCPR, CPDB etc.? Please give your suggestions with reasons.

Q.6 Should the scope of UCC regulation be enhanced to include unwanted calls like silent, obnoxious, threatening calls etc. and unauthorized communications.? What role government or constitutional organizations may play in curbing such activities? Please give your suggestions with reasons.

Q.7 What steps may be taken to address the issues arising from robo-calls and silent calls? What are the technical solutions available to deal with the issue? How international co-operation and collaboration may be helpful to address the issue? Please give your suggestions with reasons.

Q.8 For robust verification and authentication of telemarketer getting registered, what changes in the process of registration, may be introduced? Please give your suggestions with reasons.

Q.9 Should registration of other entities such as content providers, TM-SEs, Principal Entities, or any other intermediaries be initiated to bring more effectiveness? Whether standard agreements can be specified for different entities to be entered into for playing any role in the chain? Please give your suggestions with reasons.

Q.10 Whether new systems are required be established for the purpose of header registration, execution and management of contract agreements among entities, recording of consent taken by TMSEs, registration of content template and verification of content ? Should these systems be established, operated and maintained by an independent agency or TRAI? Whether agency should operate on exclusive basis ? What specific functions these systems should perform and if any charges for services then what will be the charges and from whom these will be charged? How the client database of TMSEs may be protected? Please give your suggestions with reasons.

Q.11 Whether implementation of new system should full fledged since beginning or it should be implemented in a phased manner? Whether an option can be given to participate on voluntary basis? Please give your suggestions with reasons.

Q.12 Whether scrubbing as a service model may be helpful for protection of NCPR data? Whether OTP based authentication for queries made by individuals on NCPR portal may be helpful to protect NCPR data? What other mechanisms may be adopted to protect the data? Please give your suggestions with reasons.

Q.13 What interface and functionality of NTR system may be made available to Principal entities for managing header assignments of their DSAs and authorized agents? How it may be helpful in providing better control and management of header life cycles assigned to DSAs and authorized entities? Please give your suggestions with reasons.

Q.14 What changes do you suggest in header format and its structure that may be done to deal with new requirements of preferences, entities, purpose? How principal entities may be assigned blocks of headers and what charges may be applied? What guidelines may be issued and mechanism adopted for avoiding proximity match of headers with well known entities? Please give your suggestions with reasons.

- Q.15 Whether voice calls should be permitted to TMSEs and how these can be identified by the customers? How intelligent network (IN) or IP Multi-media subsystem (IMS) based solutions may be useful for this purpose and what flexibility it may provide to TMSEs in operating it and having control on its authorized entities? Please give your suggestions with reasons.
- Q.16 What steps need to be initiated to restore the sanctity of transactional SMS? What framework need to be prescribed for those transactional SMS which are not critical in nature? Please give your suggestions with reasons?
- Q.17 To what extent, present gap between time when UCC complaint was made and time when this was resolved can be reduced? What changes do you suggest to automate the process? Please give your suggestions with reasons.
- Q.18 How the medium of Customer Complaint Resource Functionality (CCRF) with pre-validation of data e.g. Mobile App, Web Portal etc. may be helpful to achieve better success rate in complaint resolution process? Please give your suggestions with reasons.
- Q.19 Whether access providers may be asked to entertain complaints from customers who have not registered with NCPR in certain cases like UCC from UTM, promotional commercial communication beyond specified timings, fraudulent type of messages or calls etc.? What mechanism may be adopted to avoid promotional commercial communication during roaming or call forwarding cases? Please give your suggestions with reasons.
- Q.20 How the mobile App may be developed or enhanced for submitting complaints in an intelligent and intuitive manner? How to ensure that the required permissions from device operating systems or platforms are available to the mobile app to properly function? Please give your suggestions with reasons.

- Q.21 Should the present structure of financial disincentive applicable for access providers be reviewed in case where timely and appropriate action was taken by OAP? What additional measures may be prescribed for Access Providers to mitigate UCC problem? Please give your suggestions with reasons.
- Q.22 Whether strict financial disincentives should be levied for different types of techniques like robocall, auto-dialer calls for UCC? Please give your suggestions with reasons.
- Q.23 What enhancements can be done in signature solutions ? What mechanism has to be established to share information among access providers for continuous evolution of signatures, rules, criteria? Please give your suggestions with reason.
- Q.24 How Artificial Intelligence (AI) can be used to improve performance of signature solution and detect newer UCC messages created by tweaking the content? Please give your suggestions with reasons.
- Q.25 How the honeypots can be helpful to detect and collect evidences for unsolicited communications? Who should deploy such honeypots? Please give your suggestions with reasons.
- Q.26 Should the data from mobile app or from any other source for registering complaints be analyzed at central locations to develop intelligence through crowd sourcing? How actions against such defaulters be expedited? Please give your suggestions with reasons.
- Q.27 How the increased complexity in scrubbing because of introduction of additional categories, sub-categories and dimensions in the preferences may be dealt with? Whether Scrubbing as a Service model may help in simplifying the process for RTMs? What type and size of list and details may be required to be uploaded by RTMs for scrubbing? Whether RTMs may be charged for this service and what charging model may be applicable? Please give your suggestions with reasons.

Q.28 How the cases of false complaints can be mitigated or eliminated?

Whether complaints in cases when complainant is in business or commercial relationship with party against which complaint is being made or in case of family or friends may not be entertained? Whether there should be provision to issue notice before taking action and provision to put connection in suspend mode or to put capping on messages or calls till investigation is completed? Please give your suggestions with reasons.

Q.29 How the scoring system may be developed for UCC on the basis of various parameters using signature solutions of access providers? What other parameters can be considered to detect, investigate and mitigate the sources of UCC? How different access providers can collaborate? Please give your suggestions with reasons.

ANNEXURE-I

Key Initiatives by TRAI

1. Options for customer to exercise his preference: These regulations provide for registration of customers preferences using voice call or SMS on 1909. The customer can opt to block all commercial communication or can selectively block SMS from specified categories or can continue to get all calls/ SMS.
2. Options to customer to exercise his preference: The customer can opt to block all commercial communication or can selectively block SMS from specified categories or can continue to get all calls/ SMS. Regulation 7 provides options to customers to register to receive SMS from specified category or categories or not to receive any commercial communication.
3. Separate Number Series for Telemarketers: The regulations lay down a separate number series for telemarketers for voice calls; this will facilitate easy identification of telemarketing voice calls by unregistered customers receiving such calls.
4. A simple and easy procedure for exercising option by the customer: These regulations provide for registration of customers preferences using voice call or SMS on 1909. It has been mandated that all access providers shall intimate the registration number to customers by SMS within 24 hours. These regulations provide that the time taken for effecting registration of the telecom customers on the National Customer Preference Register shall be reduced to 7 days instead of 45 days.
5. Easy registration of the telemarketer with effective identification: TRAI had taken over the responsibility for registration of telemarketers and in this regard easy procedures have been laid down for registration through website www.nccptrai.gov.in Each telemarketer is given a unique registration number after payment of registration fee.
6. Sharing of Database: Sharing of National Customer Preference Register with service providers and telemarketers so that telephone databases can be effectively scrubbed before initiating telemarketing activities.

7. **Additional Security Deposit:** In order to ensure effective control, these regulations mandate all telemarketers to enter into an agreement with the Access Providers before any telecom resources are allocated to them. A security deposit will be collected from each telemarketer by Access Providers from which amount for default or contravention of regulations will be deducted. Telemarketers have to deposit additional security deposits as per the provisions in the regulations based on number of defaults or contraventions. The regulations also mandate that all telecom resources shall be disconnected at the sixth violation.

SN.	Violations(Access Provider-wise)	Deduction from Security Deposit	Security Deposit	Additional Security Deposit
1	-	-	Rs. 50,000	-
2	1 st	Rs. 25,000	Rs. 25,000	Rs. 1,00,000
3	2 nd	Rs. 75,000	Rs. 50,000	Rs. 1,50,000
4	3 rd	Rs. 80,000	Rs. 1,20,000	Rs. 4,00,000
5	4 th	Rs. 1,20,000	Rs. 4,00,000	-
6	5 th	Rs. 1,50,000	Rs. 2,50,000	-
7	6 th	Rs. 2,50,000	-	-
8	Above 6	Black listing for 2 year	-	-

8. **Blacklisting Provision:** After sixth violation apart from disconnection of telecom resources of defaulting telemarketers, provisions for blacklisting of telemarketers is also there to ensure that they do not get any telecom resources from any other access provider. The blacklisted Telemarketers will be identified through their PAN and/or TAN number. Further, access providers shall ensure that no telecom resources are allotted to such blacklisted telemarketers. Blacklisting shall be valid for a period of two years counted from the date of the disconnection of telecom resource and blacklisted companies, individuals and entities will not be provided any telecom resources across the country during this period. These measures are expected to inculcate a greater sense of responsibility among the telemarketers.

9. **Simplified Scrubbing Process:** Provisions have been made in the regulations to simplify the scrubbing process. All registered telemarketers and Access Providers are permitted to download the complete National Customer Preference (NCP) data from the NCPR website under a unique user name and password.

10. Filtering of Call & SMS by Access Provider: Filtering and auto-blocking of calls and SMS to customers according to their options: Provisions have been made such that all telemarketers ensure scrubbing of numbers using their own arrangement and all Access Providers ensure filtering of unsolicited commercial calls and SMS so that no call or SMS is sent to any customer registered on NCPR unless he has opted for it.
11. Separate Telecom Resource for Promotional Message and Transactional Message: The regulations provide a well-defined process for sending promotional messages and transactional messages through separate telecom resources dedicated for the purpose by Access Providers. Promotional messages means message containing promotional material or advertisement of a product or service. Transactional message means SMS sent by Banks, Financial Institutions, service providers, insurance company, credit card company, depositories registered with SEBI, DTH Operators to its customers pertaining to its accounts, information given by airlines or railways or its authorised agents to passengers, information given by recognised educational institutions to students or parents/ guardians, information sent by e-commerce agencies to its customers, information sent by registered companies to its employees or customers etc.
12. Specified SMS Header: In order to facilitate options for receiving SMS of predefined category or categories by customers, the regulations also define the structure of header. Customers can identify promotional SMS just by looking at the SMS header. This will reduce the inconvenience of even those customers who are not registered on the NCPR.
13. Provisions for Disconnection and Blacklisting in case Telemarketing Activities from Unregistered Telemarketers: In order to curb unsolicited commercial communications being sent by unregistered telemarketers, the regulations prescribe disconnection of telecom resources of an unregistered telemarketer by the service provider on receipt of a valid complaint, followed by blacklisting of his name and address for a period of two years. Upon blacklisting, all the other telecom resources availed by him from all service providers in the blacklisted address will also be disconnected.
14. Effective Complaint Redressal: For effective redressal of customer complaints relating to Unsolicited Commercial Communication (UCC), regulations have prescribed a framework in which action is to be taken within seven days of lodging the complaint and the customer is to be informed about the action taken. Complaint registration process has been simplified.
15. Re.0.05 Promotional SMS Charges: The Authority vide seventh amendment to the regulations has prescribed a promotional SMS charge of Re.0.05 (five paisa only) payable

by an Originating Access Provider to the Terminating Access Provider for each promotional SMS sent by a registered telemarketer from the network of the Originating Access Provider to the network of the Terminating Access Provider. This is to prevent the telemarketers from dumping promotional SMSs which results in inconvenience to consumers as well as networks.

16. Re.0.05 Transactional SMS Charges: The Authority vide Eleventh amendment to the regulations has prescribed 'a transactional SMS charge' of Re.0.05 (five paisa only) payable by an Originating Access Provider to the Terminating Access Provider for each transactional SMS sent from the network of the Originating Access Provider to the network of the Terminating Access Provider. This is to prevent the large traffic imbalance between different networks on account of transactional SMSs. Govt. agencies have been exempted from such transactional SMS charge of Re.0.05 (paisa 5 only).
17. Blocking of bulk international SMSs: Incidences came to the notice of the Authority that promotional SMS were getting routed through the international routes and were getting delivered to customers registered on NCPR irrespective of the time. Accordingly, a direction was issued on 20.01.2012 directing all Access Providers and International Long Distance Operators to ensure that-
 - no incoming international SMS containing alphabet header or alphanumeric header as a Calling Line Identification is delivered through its network;
 - no incoming international SMS containing the originating country code +91 is delivered through its network;
 - except on 'blackout days' as provided in clause (k) of sub-regulation (2) of regulation 20 of the regulations, no incoming international SMS from any source or number, originating more than two hundred SMS per hour, having similar 'signature', is delivered through its network;
 - global titles of only the network of those entities with whom the Access Providers have entered into agreement are allowed in its network.
18. Disconnection of resources of registered telemarketer: As per the principal regulations, once a telemarketer is blacklisted, every Access Provider shall disconnect the telecom resources provided by it under the regulations to such telemarketer. However, with regards to the importance of transactional messages to the telecom consumers, the Authority considered that in case a telemarketer is blacklisted for sending Unsolicited Commercial Communications through promotional resources, the disconnection of all the resources procured by him from Access Providers including the transactional resources would cause

inconvenience to the consumers. Accordingly, ninth Amendment to the principal regulations was issued on 14.5.2012 stating that in case a telemarketer is blacklisted for sending UCC through promotional resources, the telecom resources provided to it for sending promotional messages shall only be disconnected, however, in case the telemarketer is blacklisted for sending unsolicited commercial communications through the telecom resources allotted to it for sending transactional messages, the telecom resources provided to it for sending transactional messages and promotional messages shall be disconnected.

19. Measures to address UCC by unregistered Telemarketers: The Telecom Commercial Communications Customer Preference (Tenth Amendment) Regulations, 2012 dated 05.11.2012 has been issued to further tighten the regulatory framework, especially relating to commercial SMS from unregistered telemarketers. Some of the provisions of these regulations are:-

- The service providers have been offering a large number of concessional SMS packs and tariff plans for bulk SMS users. These SMS packs and tariff plans have been misused by unregistered telemarketers to send promotional SMSs to consumers. To prevent unregistered telemarketers from misusing such SMS packs or tariff plans for sending bulk promotional SMSs, a price restraint has been placed on sending of more than one hundred SMS per day per SIM at a concessional rate. The subscriber is free to send SMSs beyond this number, however, all such SMSs sent beyond one hundred SMS per day per SIM shall be charged at a rate not lower than the rate prescribed by the Authority. The Authority through the Telecommunication Tariff (Fifty Fourth Amendment) Order, 2012 dated 5th November, 2012 has prescribed a tariff of minimum fifty paise for such SMSs beyond the limit of 100 SMS per day per SIM. The changes effected by the regulations and the order have to be implemented within fifteen days.
- To restrict unregistered telemarketers from sending bulk promotional SMSs using software applications, Access Providers have been mandated to put in place a solution, which will ensure that no commercial SMSs are sent having same or similar characters or strings or variants from any source or number. The solution will ensure that not more than 200 SMSs with such similar signature are sent in an hour. However, registered telemarketers, transactional message sending entities and telephone numbers exempted by the Authority are excluded from this provision. Normal consumers sending non-commercial SMSs will also not be affected by this measure.
- The lodging of a UCC complaint through SMS has been made easier. Now the complaint can be lodged through SMS by simply forwarding the UCC SMS to 1909 after appending the telephone number and date of receipt of the SMS. Access providers

will also establish a web-based complaint registering system and a dedicated e-mail address to receive such complaints on UCC.

- For increasing consumer awareness and to caution against misuse, Access Providers have been mandated to send SMS to all customers on periodic basis, advising them not to send any commercial communications and informing them about the consequences of misuse.
- Whenever a new customer is enrolled for service, the Access Provider is required to take an undertaking from such customer in the Customer Acquisition Form that he shall not use the connection for telemarketing purpose and in case he uses the connection for telemarketing purposes such connection shall be liable to be disconnected. The regulations were further amended to address the issue of UCC from unregistered telemarketers, which was the main contributor for UCC, prescribing the following:-
- No subscriber, who is not registered with the Authority as a telemarketer, is allowed to make any commercial communication. In case it is found, based on verification of a complaint, that the UCC was originated by a subscriber who is not registered with TRAI as a telemarketer, the Originating Access Provider shall disconnect all the telecom resources of such subscriber and enter the name and address of such subscriber into a blacklist for a period of two years to be maintained separately for the purpose. Upon entry in the blacklist, all Access Providers shall disconnect the telecom resources provided by it to such subscriber within twenty four hours. No telecom resources will be allotted to such blacklisted subscriber by any Access Provider. This provision has come into force from 24.06.2013 through the 12th amendment regulations.
- Since it was observed that the unregistered telemarketers were not complying with the directions and regulations issued by the Authority, it had become necessary to make the regulatory framework more stringent, so that not only the unregistered telemarketer, but the TSPs and entities engaging such telemarketers to promote their business are held accountable. All three parties are responsible for the problem of UCC. The TSPs are encouraging such activities by providing attractive SMS packages and allowing bulk/multiple connections fully aware that these will be used for telemarketing activities. In so doing, they are breaching the Customer Acquisition Form (CAF) directives issued by the Department of Telecommunication (the licensor). TSPs are liable to pay an amount, by way of financial disincentive, not exceeding five thousand rupees for every UCC complaint originated from their network by a subscriber who is not registered with the Authority as telemarketer.

- The organizations such as banks, insurance companies, builders etc. who engage unregistered telemarketers as agents for selling their products, fail in their responsibility to ensure compliance of the regulations and, being the principal, they are equally responsible for the non-compliance of the regulations and directions issued by the Authority to address the problem of UCC. Therefore, provisions have been made in the regulations for disconnection of all telecom resources of such organisations if they are found to be engaged in telemarketing through unregistered telemarketers. Subsequently, provisions have been made for reconnection of such telecom resources in cases, wherever the Authority was satisfied about the measures taken by such entities, on payment of a reconnection charge of Rs.500/- per telecom resource (subject to a maximum of Rs.5,00,000/-).
- Since the service provider are also responsible for misuse of telecom resources by unregistered telemarketers, the amendment regulations have also made the service provider liable for financial disincentives not exceeding Rs.5,000/- for every complaint. TRAI has been imposing financial disincentive on service providers for UCC complaints based on a slab based system, based on the number of complaints per week.

ANNEXURE-II

International Scenario

[1] Responsible entities for operation, maintenance and enforcement

- i. In Australia, a Do-Not-Call Register exists since 2007. Enforcement is performed by the Australian Communications and Media Authority (ACMA).
- ii. In UK, a Telephone Preference Service has been operated by the Direct Marketing Association since 1996, and has become a nationwide official system since 1999. The service is supervised by the Information Commissioners Office (ICO). It is noteworthy that there also exists a system for registration of corporate numbers, the Corporate Telephone Preference Service (CTPS).
- iii. In Singapore, a Do Not Call Registry has been operated since 2014. The registry is operated and enforced by the Personal Data Protection Commission (PDPC).
- iv. In Korea, a system for registration of refusals has been operated since 2014. The system is enforced by the Fair Trade Commission (local authorities are also granted some enforcement competences).
- v. In France, the new nationwide Bloctel started operating from June 2016. Its operation has been assigned to Opposetel, a company composed of four telemarketing companies, and enforcement is carried out by the DGCCRF.
- vi. In Italy, the Registro Pubblico delle Opposizioni was introduced in 2011. Its operation has been assigned to the Fondazione Ugo Bordoni by the Ministry of Economic Development Department of Communications through a service agreement.
- vii. In Norway, the Reservasjons registeret has been operated since 2001, by a government registration organization called Brnny sund registrene.

- viii. In the Netherlands, a voluntary registry was being operated by Stichting Infilter, and in 2009, a nationwide official registry called Bel-me-niet Register was introduced, operated by the same organization.
- ix. In Belgium, in March 2013 the nationwide official list Nemappelez plus was introduced. The list is operated by the non-lucrative organization DNCM (which stands for Do Not Call Me), established by BDMA.
- x. In Spain, a Robinson List has been functioning since 2009. It is operated by ADIG-ITAL, an organization formed by businesses. Enforcement is carried out by the Data Protection Authority. In Switzerland, Sweden, Finland, and Portugal the list is operated by business organizations. These lists are not compulsory like but voluntary. This means that only businesses that are members of the relevant organizations are bound by such lists.

[2] Customer preference registration

- i. EU member states are free to choose between an opt-in and an opt-out system. This has led to a variation in the regulation systems, with some countries adopting a nationwide opt-out system (U.K., France, Italy etc.), some having a voluntary opt-out system run by business organizations etc. (Switzerland, Sweden, Finland etc.) and others adopting an opt-in system that is stricter for businesses (Germany, Austria, Luxembourg etc.)
- ii. In Norway, when registering, it is possible to exempt telephone solicitations for charities.
- iii. In the Netherlands, apart from natural persons, some types of legal entities can also register their numbers. When registering, it is possible to choose to refuse from among ten business categories of telephone solicitation. Telephone solicitation having as its purpose the transmission of thoughts or charity is also subject to refusal.
- iv. In Belgium, system allows for refusal of telephone solicitations even when there is an existing customer relationship. Further, legal entities can also register their numbers, and telephone numbers that are no longer in use etc. are automatically deleted from the list.
- v. In Germany, Austria, Luxembourg, and Denmark have adopted an opt-in system, where unrequested telephone solicitation is allowed only in cases where the person to be solicited has previously given its consent to such solicitation.
- vi. In Denmark, in principle adopts an opt-in system, there exist at the same time some categories of unrequested telephone solicitation that are exempted and allowed, namely

- ordering of books
- subscriptions for newspapers, magazines, and periodicals
- brokering of insurance contracts etc. and
- Subscriptions for rescue services or medical transport.
- However, an opt-out list is available for persons who wish to refuse such solicitations too.

[3] Exemptions for entities

- i. In Canada, registered charities, political parties and candidates, opinion polling firms or market research firms conducting surveys, newspapers calling to sell a subscription, and organizations that have a business relationship with the person registered are exempted.
- ii. In USA, political calls, charitable calls, debt collection calls, information calls, telephonic survey calls, calls to registered users with whom recently done business or to whom given written permission.
- iii. In Australia, exceptions from the prohibition are allowed for certain public interest organizations, such as charities, educational institutions, social researchers, opinion pollsters, and government bodies to make specific telemarketing calls.
- iv. In Singapore, charity calls, market researches etc. are exempted.
- v. In South Korea, political parties, solicitation of insurance transactions etc. are exempted.
- vi. In France, solicitations by companies with existing transaction relations, solicitations for newspapers, magazines etc. are exempted.
- vii. In Norway, Companies with whom there exists a customer relationship are exempted, as long as the objective of the telephone solicitation is the goods or services that formed the basis of such relationship.
- viii. In the Netherlands, companies with whom there is a customer relationship, market research calls etc. are exempted.

[4] Action in case of non compliance

- i. In Canada, the CRTC may impose a penalty of up to CAD 1,500 per violation for individuals and up to CAD 15,000 per violation for corporations.

- ii. In USA, those who violate the registry can be fined up to USD 40,000 per violation.
- iii. In Australia, the amount payable in case of an infringement notice ranges up to AUD 110,000 for each day on which contraventions occurred, and penalties as a result of court action range up to AUD 220,000 for each day on which infringements occurred.
- iv. In UK, violations are sanctioned with fines of up to £ 500,000.
- v. In Singapore, violations are sanctioned with penalties of a maximum of SGD 10,000.
- vi. In South Korea, violations are sanctioned with a maximum of KRW 10,000,000.
- vii. In France, Violations are sanctioned with an administrative penalty of a maximum of €15,000 for individuals and €75,000 for legal entities.
- viii. In Belgium, sanctions against violations are imposed by the Ministry of Finance.
- ix. In Spain, Violations are sanctioned with penalties of between €40,001 to €300,000.

ANNEXURE-III

Telemarketer Statistics

S.N	Description	
1	Number of Telemarketers registered (as on 15.10.2016)	11,350
2	Number of Subscribers registered in National Customer Preference Register. (as on 15.10.2016)	23.54 Crores
3	Total complaints received by service providers (From 27.9.2011 to 15.10.2016)	14,01,609
4	Number of notice sent to unregistered telemarketers (From 27.9.2011 to 24.05.2013) & (before 12 th Amendment)	2,86,910
5	Number of Telephone disconnections of unregistered telemarketers (From 27.9.2011 to 02.10.2016)	10,91,645
6	Number of notices sent to telemarketers with deduction in their security deposit and total amount deducted so far (From 27.9.2011 to 15.10.2016)	458,2.78 Crores
7	No. of Telemarketers Blacklisted (From 27.9.2011 to 15.10.2016)	14
8	No. of service providers on which financial disincentive is imposed and total amount collected so far (From 27.9.2011 to 25.07.2016)	Rs 13,17.62 Crores
9	No. of unregistered Telemarketers blacklisted for 2 years till 15.10.2016	3,39,969

List of Figures

- 1.1 Year-wise trend of UCC Complaints 4
- 1.2 Present UCC Ecosystem 6
- 2.1 UCC Registration Process 11
- 3.1 Chain of Entities Involved 27
- 3.2 UCC Ecosystem(New Entities) 39
- 4.1 UCC Complaint Resolution Process(OAP side) 47
- 4.2 UCC Complaint Resolution Process(TAP side) 49

List of Abbreviations

3GPP 3rd Generation Partnership Project.

CAF Customer Acquisition Form.

CCRF Customer Complaint Registration Facility.

CDR Call Detail Record.

CPRF Customer Preference Registration Facility.

DoT Department of Telecommunications.

eKYC e-Know Your Customer.

FD Financial Disincentive.

IMS IP Multi-Media Sub-system.

ITU International Telecommunication Union.

IVRS Interactive Voice Response System.

LSA License Service Area.

MNP Mobile Number Portability.

NCPR National Customer Preference Register.

NTR National Telemarketer Register.

OAP Originating Access Provider.

OTP One Time Password.

PCPR Provider Customer Preference Register.

RTM Registered Telemarketer.

SMS Short Message Service.

TAP Terminating Access Provider.

TCCCPR Telecom Commercial Communications Customer Preference Regulations.

TMSE Transactional Message Sending Entities.

TRAI Telecom Regulatory Authority of India.

TSP Telecom Service Provider.

UCC Unsolicited Commercial Communications.

URN Unique Registration Number.

USSD Unstructured Supplementary Service Data.

UTM Unregistered Telemarketer.

References

- [1] 3GPP TR 33.937. *Study of mechanisms for Protection against Unsolicited Communication for IMS (PUCI)*.
- [2] ACMA. *Bulk applications for donotcall registry*. Accessed: 11.09.2017.
URL: <https://www.donotcall.gov.au/consumers/bulk-applications-register-remove-check/bulk-applications/>.
- [3] *Décret n° 2015-556 du 19 mai 2015 relatif à la liste d'opposition au démarchage téléphonique*. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030617221&categorieLien=id>.
- [4] FCC. *Consumer Alert 'CAN YOU HEAR ME' SCAMS*. Accessed: 11.09.2017.
URL: https://apps.fcc.gov/edocs_public/attachmatch/DOC-344083A1.pdf.
- [5] OFCOM. *Nuisance calls and messages: Abandoned and silent calls*.
Accessed: 11.09.2017. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0018/8523/silent-calls.pdf.
- [6] TRAI. *National Customer Call Preference Registry*.
URL: <http://www.nccptrai.gov.in/>.
- [7] TRAI.
Telecom Commercial Communication Customer Preference Regulations (TCCCPR).
<http://traai.gov.in/sites/default/files/201205301159277252627regulation1dec2010.pdf>. 2010.
- [8] ITU Recommendation X.1246.
Technologies involved in countering voice spam in telecommunication organizations.