tanla

Combating Unsolicited Commercial Communication and the systemic issues.

EMPOWERING CHOICES.

MWC19™ Barcelona

25-28 February 2019

tanla.com

TABLE OF CONTENTS

Executive Summary 1

Nielsen Survey 2

CHAPTER 01

The World of Commercial Communication 8

Nielsen Survey Results 9

1.1 Introduction 11

1.2 Modern Channels of Commercial Communication - Content Finds Customer 15

1.3 The prominence of Commercial Communication - The Rise of A2P 19

1.4 Key Players in the Ecosystem 21

CHAPTER 02

The Advent of Unsolicited Commercial Communication 27

Nielsen Survey Results 28

2.1 Overview of UCC 29

2.2 Types of UCC 29

2.3 Case Studies 38

CHAPTER 03

Regulatory Landscapes Across the Globe 41

Nielsen Survey Results 42

3.1 Global Regulatory Landscapes 49

3.2 The Indian Context 51

3.3 The Telecom Commercial Communications Customer Preference Regulation 2018 55

CHAPTER 04

The Indian Case Study 59

4.1 The Regulatory Initiative 61

4.2 Tanla's Pioneering Solution 62

4.3 What's in it for all the Stakeholders 65

The Way Forward 67

Glossary 69

References 71

About Tanla 73

FOREWORD

D. Uday Kumar Reddy

Chairman

As Tanla, we are extremely customer centric and our focus remains on enhancing customer experience and minimising spam, fraud and privacy breaches. Along with this we are committed to restrict unregistered entities that promote UCC thereby increasing the efficiency of the value chain and building greater trust in the ecosystem.

Businesses today are looking for channels to interact with their customers, in ways that are cost-effective while ensuring enhanced coverage and hyper personalisation. With increasing adoption of new-age technologies, commercial communication has enabled enterprises across sectors and geographies to effectively achieve the aforementioned and connect with their customers to significantly expand their business.

Commercial communication using Application to Person messaging happens to be the most prolific medium globally and is estimated to grow from 1.7 trillion in 2017 instances currently to about 2.7 trillion by 2022. In order to make these predictions a reality, it is important to ensure sustained coherence within the ecosystem. For persistent growth it is important have ensure coherence within the ecosystem. It would also be imperative to have all stakeholders governed by progressive policies and regulations while safeguarding the interests of the consumers.

Through commercial communication, various enterprises have been successful in gathering massive volumes of customer data. While enterprises try to guard this data with utmost care, there have been increasing instances where such data has been exploited through unethical means for revenue generation and customer privacy and consents have not been honoured. Unsolicited Commercial Communication (UCC) is a concern and due to this, many customers have increasingly fallen prey to spams, phishing and frauds thereby impacting the user experience and also the trust in the ecosystem.

Globally regulators have tried with varying degree of success to ensure that customers are safeguarded from UCC and subsequent frauds and privacy breaches through various means. This includes introducing various regulations, defining penalties, driving customer awareness programs etc. However in the absence of technology to monitor such initiatives, it has been increasingly difficult to ensure a high degree of compliance and customers still are subject to spam and phishing. In this context, the recent regulation issued by the Telecom Regulatory Authority of India i.e. the "Telecom Commercial Communications Customer Preference Regulations, 2018", is a welcome step in order to drive compliance and create a cleaner ecosystem for all the participants. The regulation is particularly pathbreaking as it envisages using technology significantly to complement and enable the regulatory objectives. Use of Distributed Ledger technology along with modules on machine learning and artificial intelligence would allow greater accountability and fraud detection capabilities.

As Tanla, we are extremely customer centric and our focus remains on enhancing customer experience and minimising spam, fraud and privacy breaches. Along with this we are committed to restrict unregistered entities that promote UCC thereby increasing the efficiency of the value chain and building greater trust in the ecosystem. In line with our underlying mission of 'No Spam, No Fraud, Yes Privacy,' Tanla is glad to introduce the world's first blockchain enabled commercial communications stack to curb UCC– Trubloq. As a market leader, Tanla has been efficacious in building consensus among the key players in the ecosystem while meeting all the regulatory requirements to develop a wider use case for Trubloq. As the market leader, Tanla has taken the initiative for spreading awareness about the regulation and its benefits through surveys, workshops, road shows and training programs. Tanla is determined to drive the vision of the regulator and bridge any gaps that arise between the stakeholders and regulators.

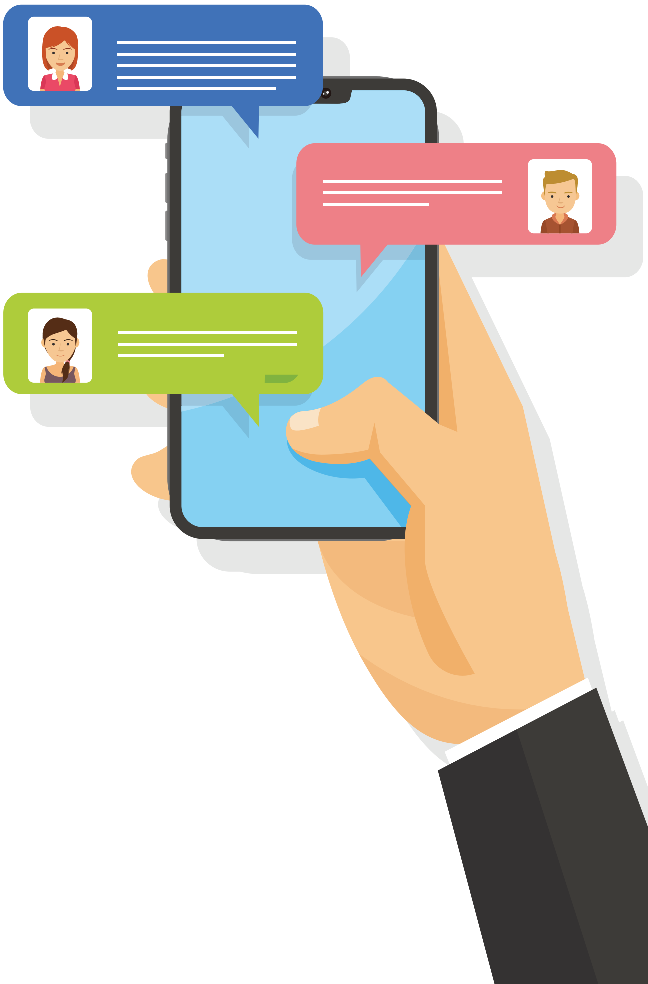
Our platform's multidimensional architecture focuses not only on transactions but also on building accountability. By leveraging "Machine Learning and Artificial Intelligence" we are able to identify patterns to flag fraudulent behaviour, eliminate unregistered entities and ensure data privacy. This unique blend of regulation with innovation and technology to control the volume of UCC would make way for a highly disciplined and trusted commercial communication ecosystem.

This report aims to highlight the avenues and the immense potential of commercial communication and how technology used wisely with regulations is an exponential use case for the benefit of all the stakeholders in the ecosystem. The outcome has to be in empowering the choices for all the stakeholders in the ecosystem and we are determined to succeed!

In line with our underlying mission of 'No Spam, No Fraud, Yes Privacy,' Tanla is glad to introduce the world's first blockchain enabled commercial communications stack to curb UCC – Trubloq.

EXECUTIVE SUMMARY

Communication is an underlying aspect to majority of business expansion strategies. Businesses today, have transformed and have a more customer centric outlook, with marketing of their products being one of the most critical agendas. Advancements in technologies has allowed for businesses to augment their products to cater to the customer needs while ensuring profitability which further creates the need for customers to be aware of these products. In this regard, businesses were quick to realise the potential of telecommunication services such as voice calls, SMS and internet based communications such as SMS, instant messaging, emails, etc. in reaching out to the masses.



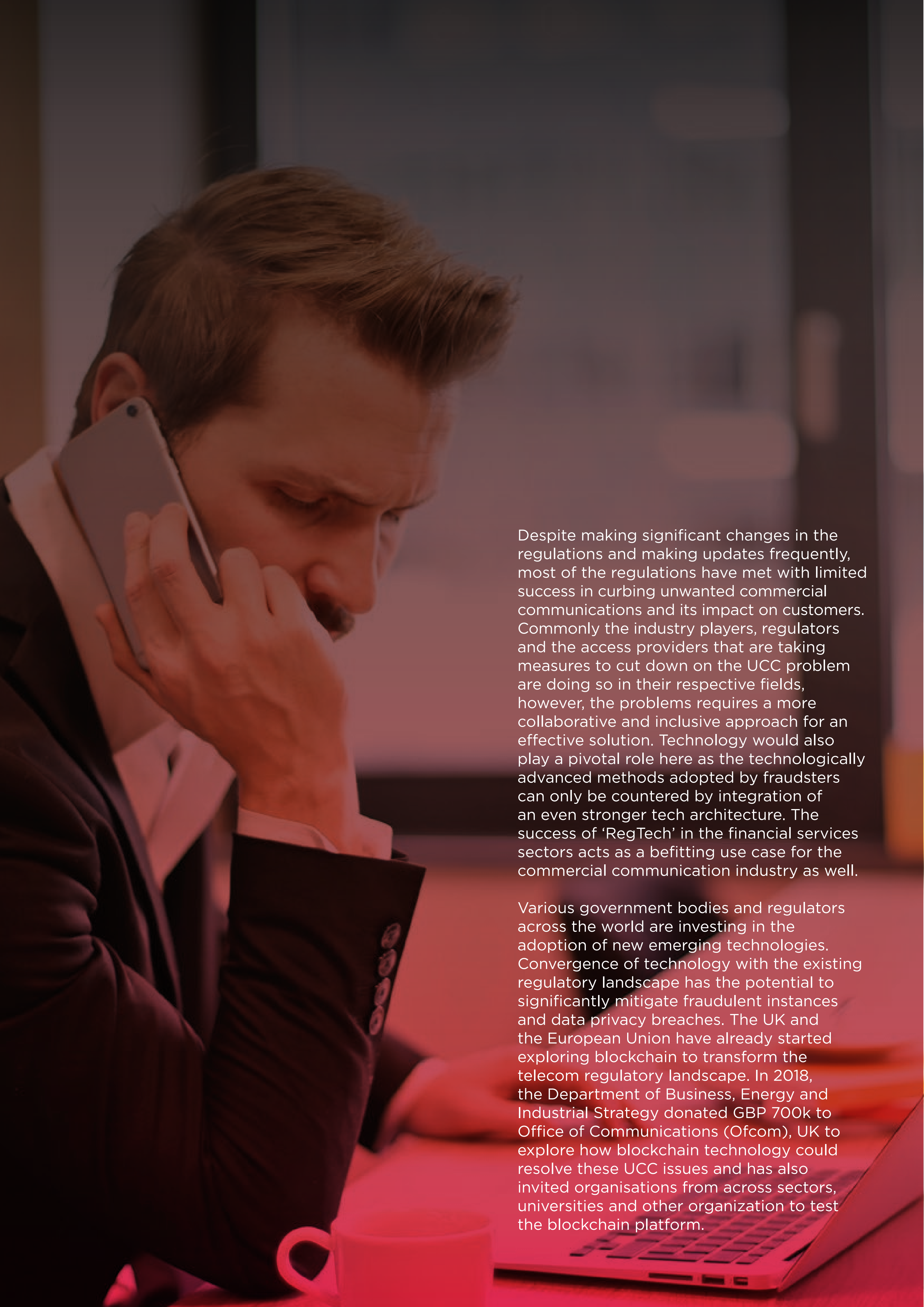
Of the 7.6 billion world population, 5 billion are unique mobile phone subscribers with telecom services, thus, reaching out to customers through telecom channels using mobile phones as the preferred platform proved to be a ground breaking communication

Voice, messaging and emails are becoming increasingly relevant as they drive commercial communication beyond the conventional boundaries such as sectors, geographies, cultures and demographics. The simplicity of entering a market that too at surprisingly lower costs both in terms of money and efforts through mobile messaging has paved the way for Rich Communication Services (RCS) such as Application to Person (A2P) messaging (bulk messaging) to reach consumers. With the introduction of bulk messaging to customers, numerous industries across the globe such as Banking and Financial Services, E-commerce, Tourism, Logistics, etc. adopted commercial communication as their preferred channel of communications with the customers.

Unwanted and irrelevant communications are not only invading customer space but are also a very effective means for duping customers into sharing their personal and financial details (phishing), falling prey to malware attacks and various other fraudulent activities. Tracking customer's personal information, interests and behavioural patterns have given rise to an incredibly opaque data brokerage industry. Emergence of novel technologies such as automated or robocalls, sophisticated phishing and spoofing techniques, technical loopholes like grey routes and sim farms leading to numerous instances of frauds have brought tremendous stress to the global messaging ecosystem.

> **In 2017, a MobileSquared analysis reflected that USD 7.7 billion was the bulk messaging revenue lost by players to A2P frauds and leakages, for an approximately USD 12 billion dollar industry, elimiating such losses could almost double the industry size.**

While on one hand fraudsters come up with new techniques to exploit network and ecosystem vulnerabilities, regulators across the globe continue to develop or augment regulatory frameworks to create a more robust control landscape to safeguard customer interests and curb UCC. Regulatory bodies in countries such as the US, UK, EU, Canada, India, Australia, China, etc. actively participate in creating a comprehensive regulatory framework for the commercial communication ecosystem. Incorporating opt-in models, registering customer detailed and categorized consent, defining cross-border data transfers mandates, strengthening complaint handling mechanism and expediting complaint redressals and levying hefty financial penalties in case of non-compliance are some of the most common practices adopted by regulators across countries.



Despite making significant changes in the regulations and making updates frequently, most of the regulations have met with limited success in curbing unwanted commercial communications and its impact on customers. Commonly the industry players, regulators and the access providers that are taking measures to cut down on the UCC problem are doing so in their respective fields, however, the problems requires a more collaborative and inclusive approach for an effective solution. Technology would also play a pivotal role here as the technologically advanced methods adopted by fraudsters can only be countered by integration of an even stronger tech architecture. The success of ‘RegTech’ in the financial services sectors acts as a befitting use case for the commercial communication industry as well.

Various government bodies and regulators across the world are investing in the adoption of new emerging technologies. Convergence of technology with the existing regulatory landscape has the potential to significantly mitigate fraudulent instances and data privacy breaches. The UK and the European Union have already started exploring blockchain to transform the telecom regulatory landscape. In 2018, the Department of Business, Energy and Industrial Strategy donated GBP 700k to Office of Communications (Ofcom), UK to explore how blockchain technology could resolve these UCC issues and has also invited organisations from across sectors, universities and other organization to test the blockchain platform.

A classic example of adoption of the RegTech solution in the commercial communication ecosystem is that of the Telecom Regulatory Authority of India (TRAI) which re-introduced the Telecom Commercial Communication Customer Preference Regulations (TCCCPR) in July 2018.

> **India is globally the second largest telecommunication market by count of subscribers and correlatively has the highest volume of Spam calls per user per month, 22.**

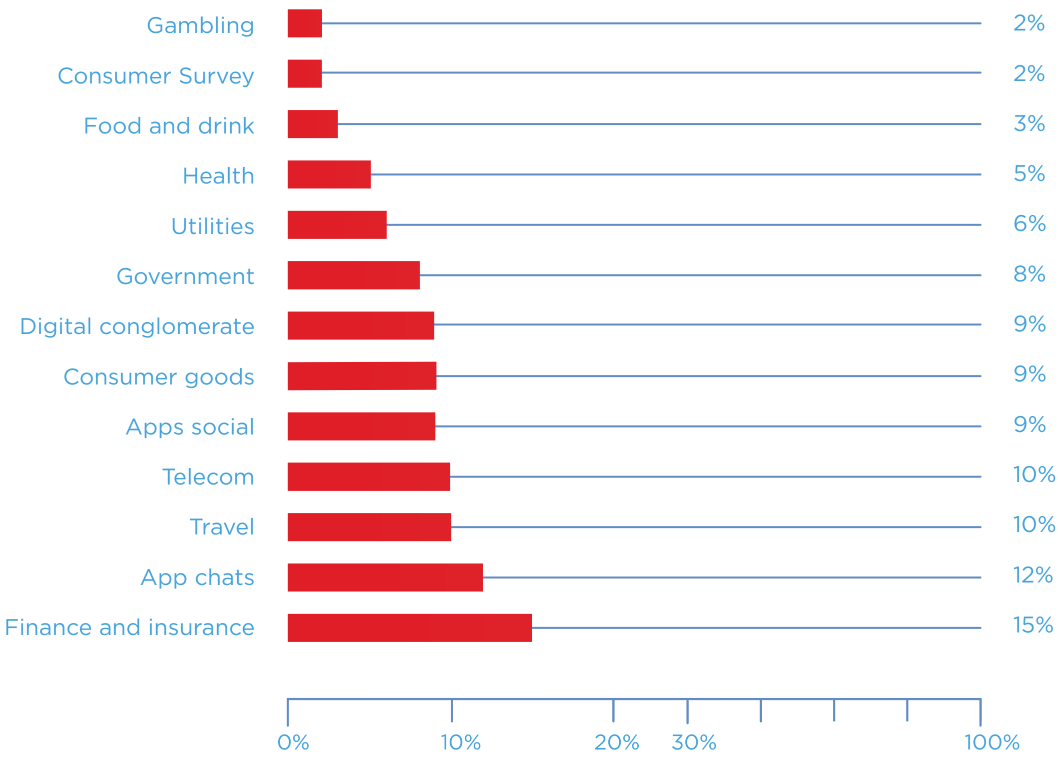
TCCCPR 2018 sets out to integrate blockchain or Distributed Ledger Technology (DLT) in the controls framework of its existing regulatory mandates.

Through DLT, the TRAI envisages to significantly enhance the customer preference and consent registration as it would reduce the overall turn around time for registration and implementation of choices by maintaining all information on distributed ledgers. It also strengthens traceability by maintaining digital records and eliminating voice or written consents. The regulation also mandates registration of senders, their header (sender names), message and voice content templates bringing immense transparency in every transaction which would drastically improve the customer complaint management and redressal system. Whitelisting all critical elements further strengthens scrubbing capabilities while securing customer information. Cumulatively, TCCCPR is now making way for a more customer centric environments wherein their needs and information security are of utmost importance.

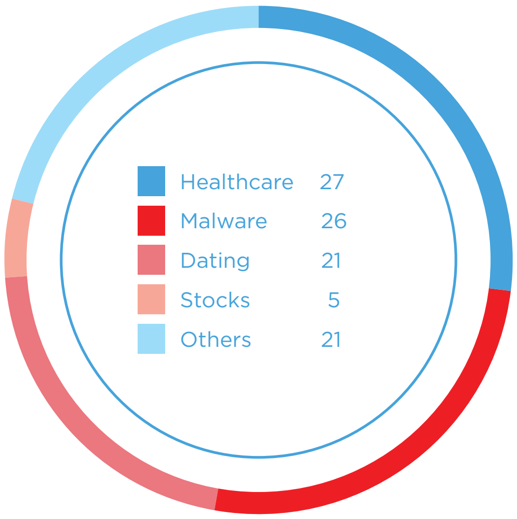
Immediately following the introduction of TCCCPR in 2018, one of India's market leader in the space of commercial communication, Tanla Solutions designed a DLT enabled solution 'Trubloq' consistent with the mandates and the recommendations laid out by the TRAI. With the underlying mission of 'No Spam, No Fraud, Yes Privacy', Trubloq is the world's first blockchain enabled solution designed to empower customer choices while maintaining a healthy commercial equilibrium among all the players. Tanla identified the need for a more collaborative and symbiotic ecosystem for which it set out to take inputs from every player in the ecosystem by conducting market research surveys, roadshows, consultancy papers and session, panel discussions, etc. Trubloq is a cryptographically secured and immutable solution that would augment security and confidentiality. It is a future ready product that is highly compatible with Artificial Intelligence (AI) and Machine Learning (ML) technologies for best in class pattern detection and self evolving capabilities.
The adoption of technological advancements by industries for developing their products invariably upgrades the entire ecosystem gradually. With these advancements, it is only logical for regulations too to upgrade and create a more relevant control landscape for there to be an equilibrium among the needs of all of the customers and the businesses.

COMMERCIAL COMMUNICATION AT A GLANCE

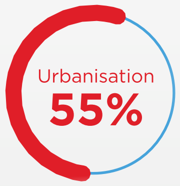
a. TOTAL A2P TRAFFIC BY SECTOR



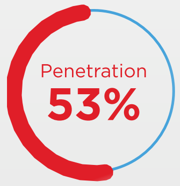
b. MOST PREVALENT SPAM CONTENT CATEGORIES WORLDWIDE IN 2017



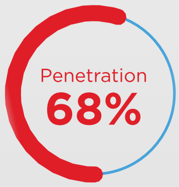
c. DIGITAL AROUND THE WORLD IN 2018



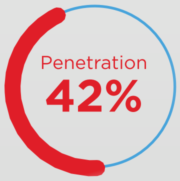
Total Population
7.593 Billion



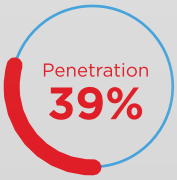
Internet Users
4.021 Billion



Unique mobile users
5.135 Billion

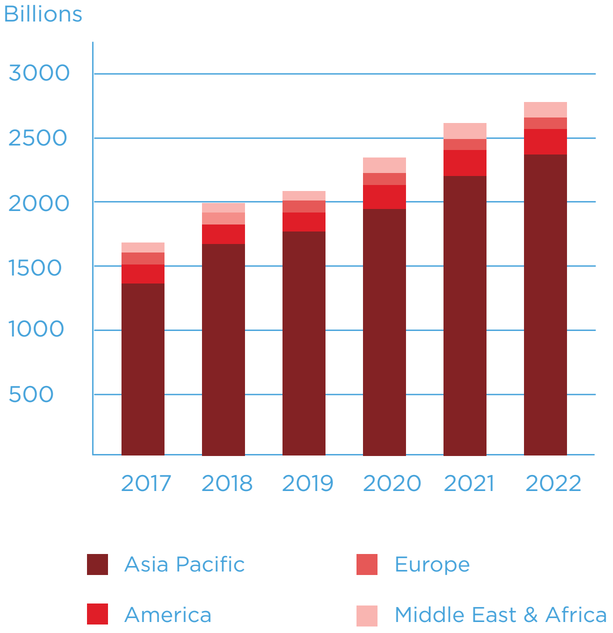


Active social media users
3.196 Billion

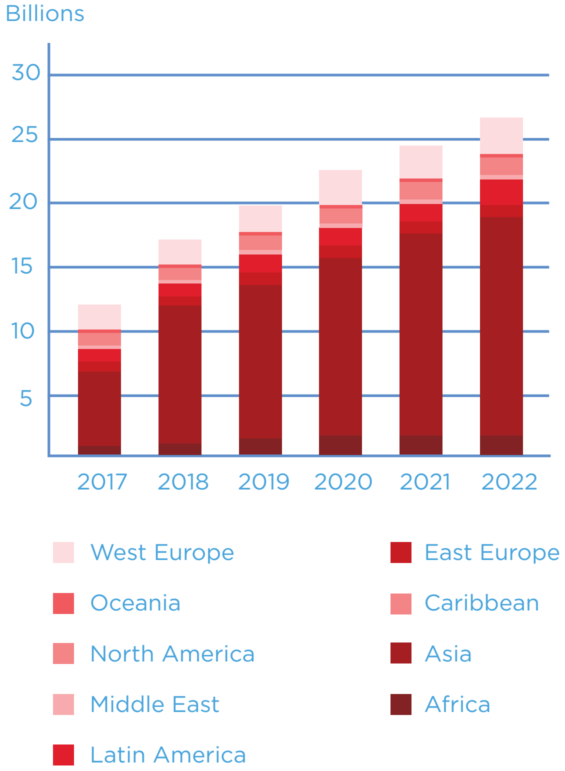


Active mobile social users
2.958 Billion

d. TOTAL GLOBAL A2P SMS MESSAGES BY REGION (2017-2022)



e. GLOBAL A2P SMS REVENUES



f. MOBILE USERS VS MOBILE CONNECTIONS GLOBALLY

Number of unique mobile users (any type of handset)- **5.135 Billion**

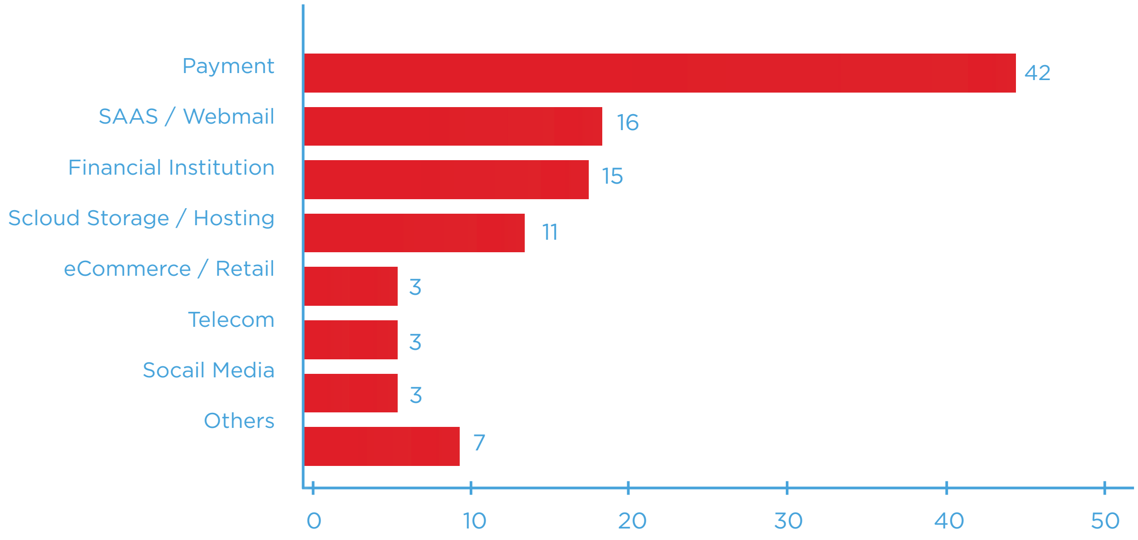
Total number of mobile connections- **8.485 Billion**

Mobile connections as a percentage of total population- **112%**

Average number of connections per unique mobile users- **1.65**

Mobile Penetration (unique users vs total population)- **68%**

g. MOST-TARGETED INDUSTRY SECTORS FOR PHISHING ATTEMPTS , Q4 2017



NIELSEN SURVEY

Determined in building consensus, understanding the importance and current perception of data privacy for consumers, Tanla Solutions commissioned a comprehensive customer survey through AC Nielsen Company. Driven to conduct awareness about the regulatory reforms in the Indian ecosystem for consumers to reap benefits from, the objective was to understand the existing knowledge users had about registering their choices and complaints. The purpose of the survey was to understand how consumers perceive the communication they receive from their brands and the inconvenience caused to them.

The survey was an online self-administered questionnaire with insights across–

- Customer commercial communication patterns
- Data privacy
- Impact on customer trust due to non adherence of customers choices
- Customer awareness about registration of choices and complaints

From a sample of more than 2000 participants with responses from 7 metro cities, 17 tier 1 cities and 58 tier 2 cities across India, the survey was an initiative to understand the growing concern of spam, fraud and user inconvenience caused to customers. A few prominent insights from the survey were -

- Most customers prefer commercial communication through SMS and calls over OTT channels
- Consumers prefer to receive communication about their financial engagements, followed by ecommerce and entertainment
- On an average consumers receive up to **9** unwanted messages or calls daily
- Given the high number of unwanted messages and calls, **97%** consumers feel that data privacy is important to them
- **6 in 10** consumers consider Data Privacy an important aspect of commercial communication
- On average, consumers are ready to pay **12 INR** monthly to secure their data
- About **2 in 3** people have complained their mobile operator about unwanted calls messages
- Nearly half of the consumers are also not aware of new regulations to curb unsolicited communication

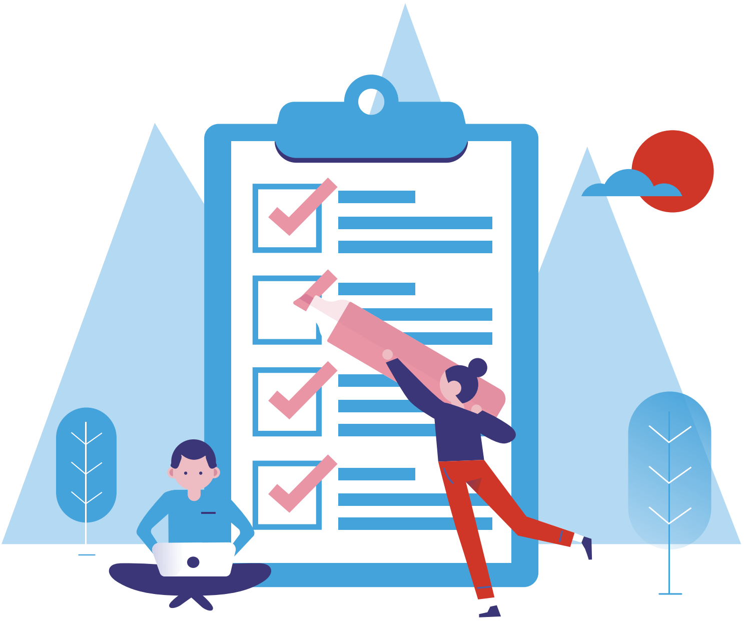
Nielsen, a leading global information & measurement company, provides market research, insights & data about what people watch, listen to & buy.

AGE GROUP	
18 - 25 years 26 - 45 years Above 45 years	988 931 84
GENDER	
♂ Male	1342
♀ Female	661

1

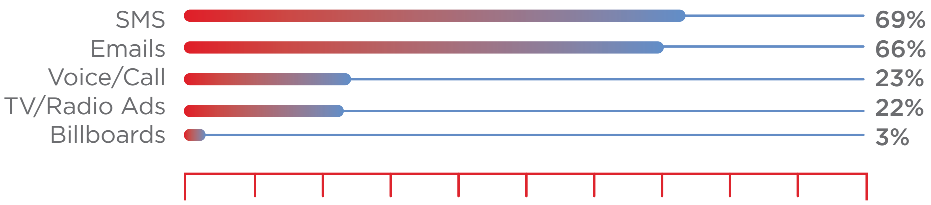
THE WORLD OF COMMERCIAL COMMUNICATION

NIELSEN SURVEY RESULTS



BEST WAY TO RECEIVE COMMUNICATION FROM FAVOURITE BRAND

Q1. What is the best way for you to receive communication from your favorite brands ? [You can select upto 2 responses]

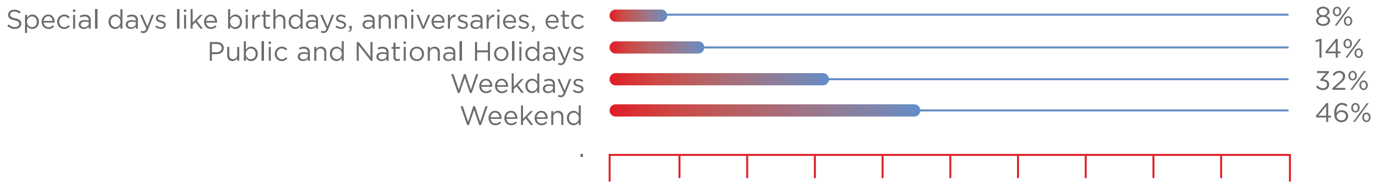


Once they have given consent, **SMS and Emails** are the preferred mode of communication from brands, **SMS is preferred by females**

emails are preferred by middle aged and metro consumers (possibly due to greater internet penetration)

WHEN TO COMMUNICATE...

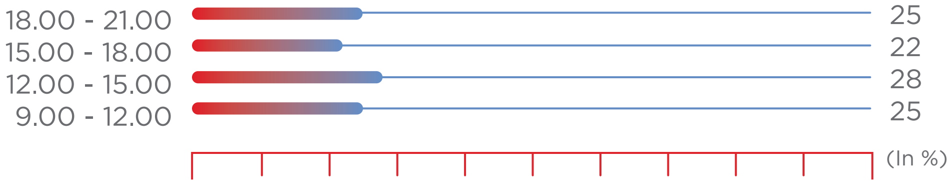
Q5. What day type would you prefer to receive commercial communication?



Weekend is the most **preferred time of the week** when the consumers would like to receive commercial communication

WHEN TO COMMUNICATE DURING THE DAY...

Q6. What time band would you prefer to receive commercial communications?

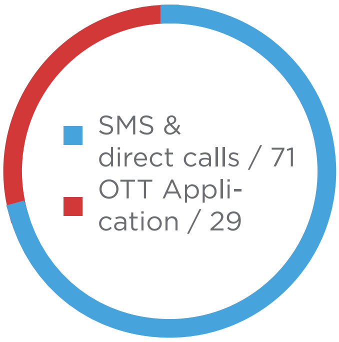


Evenings are the least **preferred time of the day** to receive commercial communication

RECEIVING COMMUNICATION IS EASY THROUGH...

Q7. In your opinion, is it easier for you to receive communications from your preferred brands through SMS, Direct Calls or through the OTT players like WhatsApp, Viber, Facebook messenger, WeChat, Telegram, etc.?

SMS and direct calls continue to be perceived as easier to receive communication



THE WORLD OF COMMERCIAL COMMUNICATION

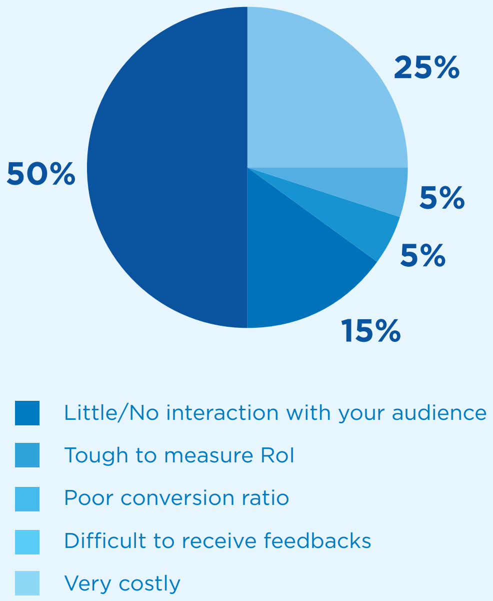
Communication with customers has become the forefront of relationship building and business development for organisations today. Commercial communication in its basic form is marketing, public relation, advertisement and transactional communication between enterprises and their end customers[1].

> **In common parlance "commercial communication" refers to message, voice or SMS, made through telecommunications service, which is transmitted for the purpose of informing about, or soliciting or promoting any commercial transaction in relation to goods, investment or services. [1]**

Commercial communication strategies are reflective of the service benefits an enterprise proposes to attract their target consumers. Effective commercial communication can create a niche position for enterprises in the minds of their existing and potential customers, thereby leading to an enhanced brand image, increase in sales and profitable financial results.

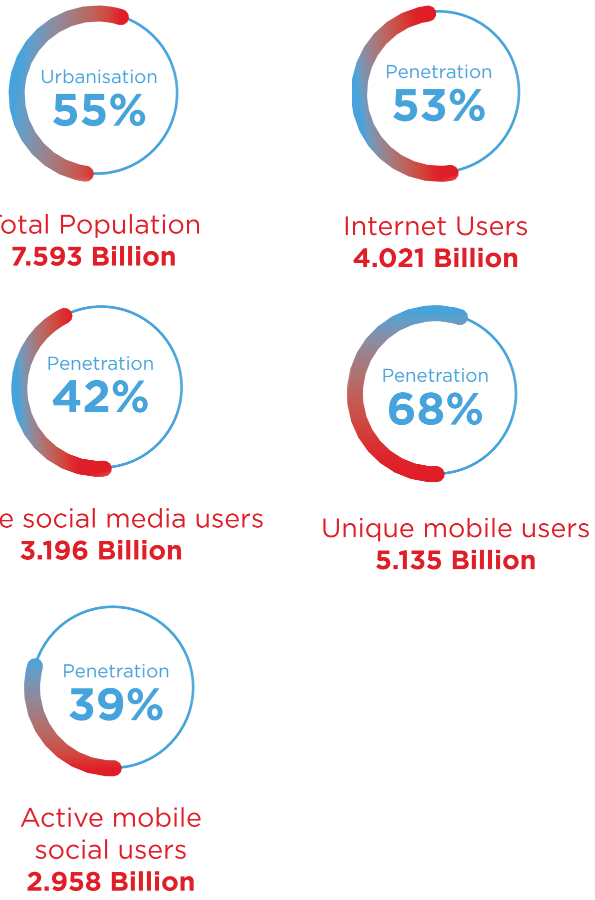
Magazines, mail order catalogues, pamphlets, newspaper, radio and television advertisements were some of the common

2 Marketers state the biggest Drawbacks of traditional marketing



traditional forms of communication that enterprises commonly used. Despite their high costs, the traditional forms were powerful methods of communication as they were able to actively reach out to the masses. The reach and scope of traditional modes of communication were often askew in aligning the brand image enhancement activities with the right budget. Limited to promotional activities, the traditional channels of communication were not lucrative investments. These channels, tapped into a large customer base but lacked critical aspects such as segmentation, personalisation and instantaneous connect. This led to poor conversion rates and low return on investment for enterprises. With technological advancements such as mobile phones and the expanse of communication services, limitations of traditional communication methods such as radio, TV, postcards, etc. have become increasingly prominent. Technology has enabled users with swifter mechanisms such as Application to Person (A2P) SMS, voice calls, emails and instant messengers. Such modern platforms have allowed users to instantly communicate, share, record and maintain a history of preferences.

3 Digital around the world in 2018

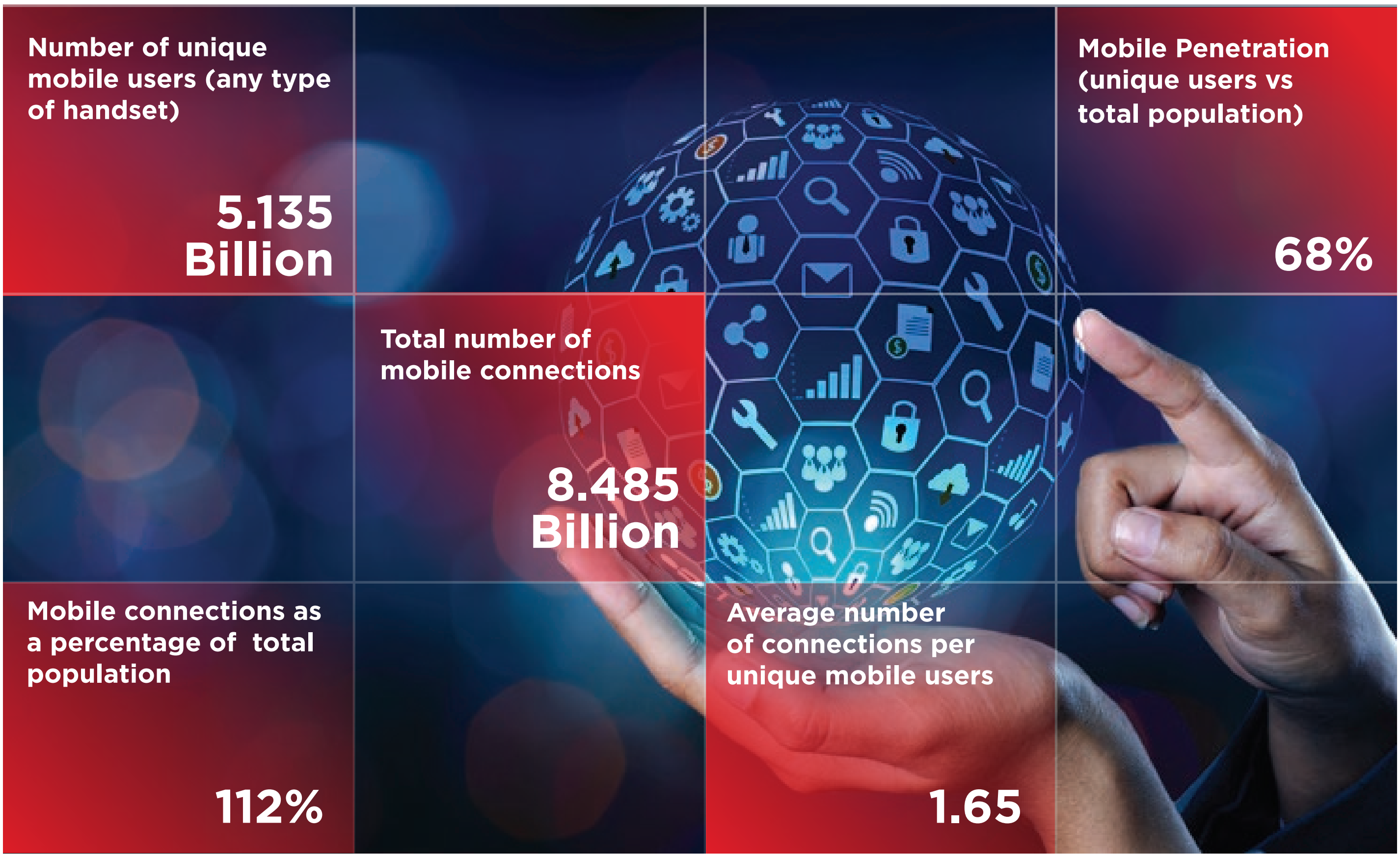

Urbanisation 55%
Total Population
7.593 Billion

Penetration 53%
Internet Users
4.021 Billion

Penetration 42%
Active social media users
3.196 Billion

Penetration 68%
Unique mobile users
5.135 Billion

Penetration 39%
Active mobile social users
2.958 Billion


Number of unique mobile users (any type of handset)

5.135 Billion

Mobile Penetration (unique users vs total population)

68%

Total number of mobile connections

8.485 Billion

Mobile connections as a percentage of total population

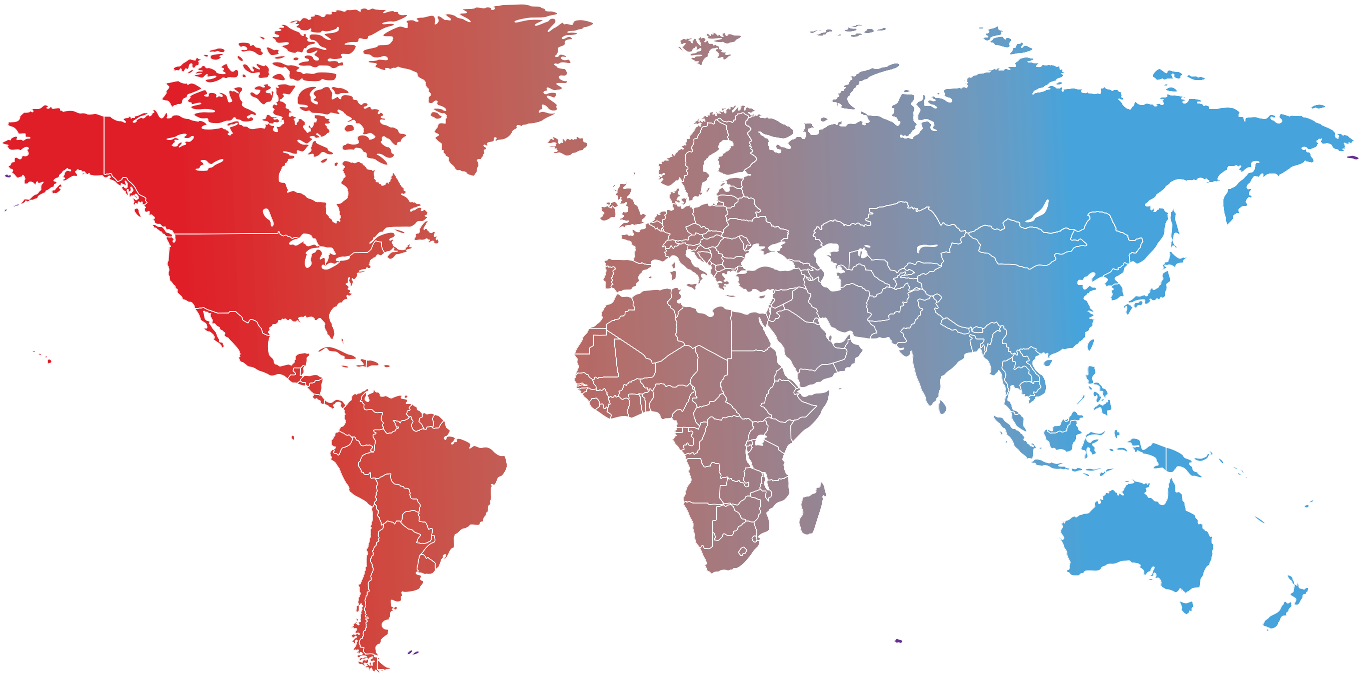
112%

Average number of connections per unique mobile users

1.65

3 Mobile Users vs Mobile Connections - Comparing the number of unique mobile users to the number of mobile connections

4 Number of unique mobile subscribers worldwide hits five billion



North America
292 M Unique Mobile Subscriber

6% 80%

Latin America
459 M Unique Mobile Subscriber

9% 71%

CIS
227 M Unique Mobile Subscriber

5% 79%

Sub-Saharan Africa
463 M Unique Mobile Subscriber

9% 44%

Middle East and North Africa
391 M Unique Mobile Subscriber

8% 63%

Europe
465 M Unique Mobile Subscriber

9% 86%

India
730 M Unique Mobile Subscriber

14% 54%

Asia Pacific
2765 M Unique Mobile Subscriber

55% 68%

Europe
465 M Unique Mobile Subscriber

9% 86%

- **Total Unique Mobile Subscribers(Million) - 5035**
- **Total Subscriber Penetration (% of population) - 67%**

🟦 Total Subscriber Penetration

🟥 % of global subscriber base

Continuous innovations in channels such as SMS, voice and emails have allowed commercial communication to cross barriers of time, geography and demographics and are continuing to aid industries and individuals worldwide. Social media platforms have reduced communication complexity in the form of short spurts such as hashtags for prompt understanding. Such evolving forms of communication have provided utmost convenience to the users by providing access to a wider information base.

» Unlike traditional forms of communication, commercial communication enables organisations to efficiently and instantly communicate with their users beyond boundaries. Today through SMS and emails, geo-targeting is easy and possible.

» The scope of commercial communication has moved beyond promotional use to incorporate transactional and service related communication within its domain. Customer interaction is not limited to promotional updates as communication today enables enterprises to communicate essential service details as well to their customers. E-Commerce websites today provide real-time logistical updates to the buyer of a product, thereby keeping them engaged and making the process more customer-centric.

» As per Ovum's Enterprise Messaging Survey 2017, SMS is a well-accepted channel by which enterprises send marketing and promotional messages, with **42%** and **35%** of respondents, respectively, indicating that their use of SMS for these purposes increased over the past year.[5]

» Hyper localization capabilities allow companies' flexibility in terms of tailor-made messages for their varied customer segments. In multilingual regions, message templates are created in various languages in order to appeal to the native customers. Such hyper-personalization abilities allow organizations to create meaningful customer relations and give their customers a feel of "personal touch."

» The wider market reach through digital forms of commercial communication, have enabled companies to drive down their cost to acquire and retain customers. Further, this has allowed organizations of all sizes to turn non-captive customers into captive customers.

> **"SMS is an important channel of communicating with our customers as we send out information on product purchases, registration, services, etc. We at KENT, believe that with TRAI's new regulation SMS communication will become more trusted and secure and will be eventually beneficial for the brand."**
>
> ***Saurabh Gupta***
> ***Chief Information Officer, Information Technology, Kent RO Systems Limited***

1.2 MODERN CHANNELS OF COMMERCIAL COMMUNICATION – CONTENT FINDS CUSTOMER

Technological advancement has allowed enterprises to increase customer touchpoints by assimilating themselves within customer behavioural patterns. Enterprises today can choose the right channels to tap their target audience and engage them in their habitual space. These evolving sources have become an essential piece in the puzzle of business success.

1.2.1 Application to Person (A2P) SMS

A2P SMS is the most pervasive channel for commercial communication. Irrespective of the type of phone used by the customer (feature phone/ smartphone) SMS services work seamlessly.

> **Boasting an open rate of 98% and a response rate of 45%, SMS stands out as the most popular mode of communication.[6]**

The use of this channel is across different industry types and is used for transactional communications, promotions, verification and password confirmations, alerts and appointment reminders, feedback, logistic tracking, customer support, etc.

Formerly, a group of industry promoters created a more immersive and interactive form of SMS, the Rich Communication Services (RCS). RCS allows the use of videos, audios, actionable buttons and 'read' receipts by its end customers thereby enabling enterprises to send more meaningful and intuitive contents to the users.

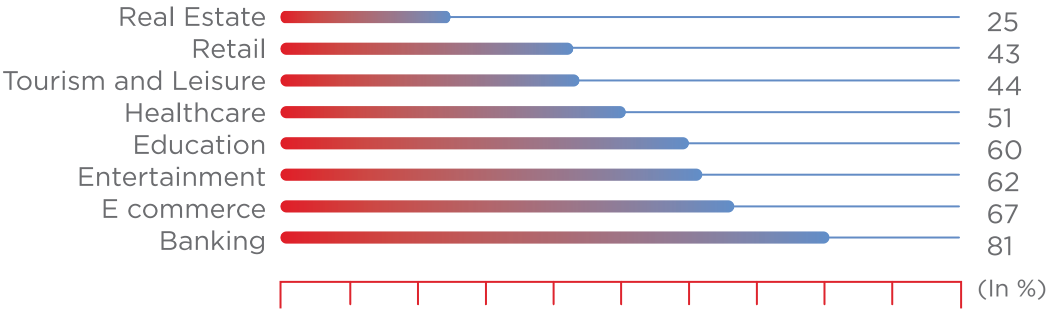
> **It is estimated that revenues from RCS messaging will exceed approx. $9 billion by 2022 from an estimated $126 million in 2018. With forecasted global RCS users of 2 billion by 2022, it is projected that over 90% of RCS traffic will be A2P by 2022.[7]**

"Bombay Stock Exchange (BSE Ltd.), Asia's 1st exchange and the fastest in the world. BSE is India's leading exchange group which relies on SMS to keep millions of investors updated about their investments and transactions. SMS is fast and effective but also prone to phishing and frauds.
We are happy to note that with TRAI's new regulation, SPAM and other unsolicited communications will be nipped in the bud and branded communication will help build trust and faith with end users."
- Amit Mahajan
Head Information Products and Procurement, SEBI

NIELSEN SURVEY

PREFERRED BUSINESS CATEGORY FOR RECEIVING MESSAGES

Q4. From which of these business categories would you like to receive messages?



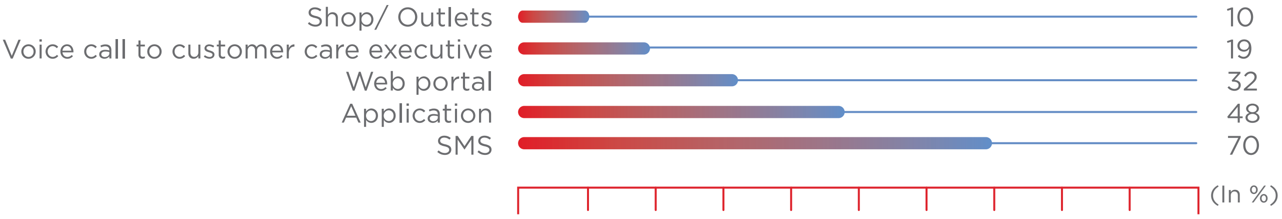
Young consumers would like to receive communication related to education

Females, consumers in metros and middle aged consumers are more open to receiving communication across sectors

Most consumers would like to receive communication from banking & e-commerce sectors

PREFERRED CHANNEL FOR TAKING CONSENT

Q3. What would be your preferred communication channel, if your favorite brands would want to take your consent to send information of their best deals, service due dates, etc.? (You can select up to 2 responses)



Consumers prefer being contacted via SMS if their brands want to take consent to send communication to them followed. Other preferred means being Apps and web portals

Consumers above 45 years of age and females are more likely to prefer SMSes

1.2.2. Email

The growing popularity of email has paved the way for enterprises to communicate effectively with their customers at limited or no cost. In 2018, approx 1.75 email accounts were held by a user.[8] Email communication is considered as a more formal platform of communication by most enterprises and widely accepted for complaint registration and redressal, promotion, user subscription, transactional confirmations and receipts, etc.

The exponential growth in smartphone subscriptions, advancement in internet speeds to 5G and easy access to smart gadgets has made it more convenient for consumers to access their emails. “Mobile users check their emails more than non-mobile users by an average of 3x as much”.[8]

Commonly used for sending promotional messages, subscription-related information, product/ service updates, this platform allows enterprises to share visually appealing content while also allowing them to add click-through links and embed videos and audio clips. As per a survey conducted by Ovum, when survey respondents were asked which alternative communications channels to SMS they use for transactional or promotional messaging, the e-mail came out as the second most favoured communication with 84% respondents.[8]

Not limited to a word limit and flexibility in terms of user appeal, email as an alternative to SMS for commercial communication is reflective in its many benefits.

» **Design**
» **Cost Efficient**
» **Shareable**
» **Measurable**
» **Non-Intrusive**

1.2.3. Voice

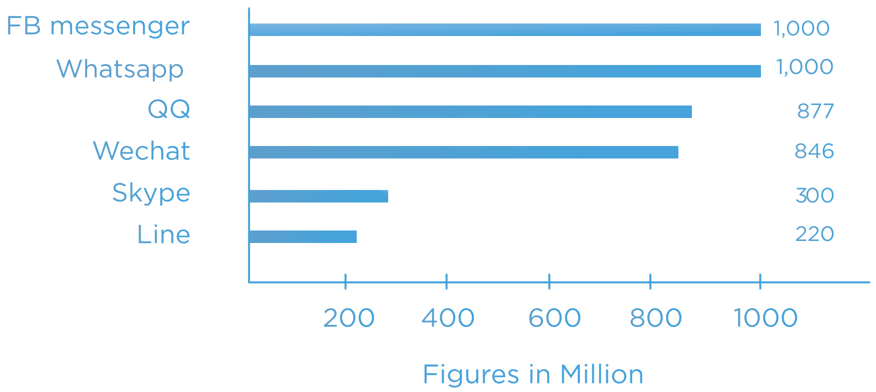
Enriched customer experience has become the focal point of all the enterprises and is growing more eminent in recent times. Enterprises have incorporated telemarketers and set-up call centres globally to understand their customer’s behaviour and address their concerns real time by leveraging the platform of voices calls.

> **Facilities such as Interactive Voice Response Systems (IVRS) have automated and further streamlined user interaction. Predominantly used for inbound calls, the pre-recorded audio (IVRS) guides the customer and enables them to communicate using the dial pad or speech recognition.**

Such systems allow calls to be answered in the first ring, reducing customer’s average waiting time. This form of personalisation is always at the customer’s disposal and can be easily adapted to suit the enterprises’ requirements.

Similar and popular channels such as robocalls are computerised auto-dialled calls made to customers that play a pre-recorded message. Predominantly used for outbound calls, robocalls can be tailored to suit the needs of the organisation and are commonly used for political campaigns and promotional messages.

9 Active users of key global social platforms



1.2.4. Over The Top (OTT)

Another emerging and popular channel of commercial communication that operators and enterprises are increasingly adopting are the OTT (Over the Top) platform.

> **Applications such as Facebook Messenger, Whatsapp, WeChat, Line, etc. with billions of active users are proving to be an increasingly adopted channel for commercial communication.**

Travel companies, airlines, hospitality chains are using such channels to intimate travel details, PNR details, booking confirmations, movie tickets etc.

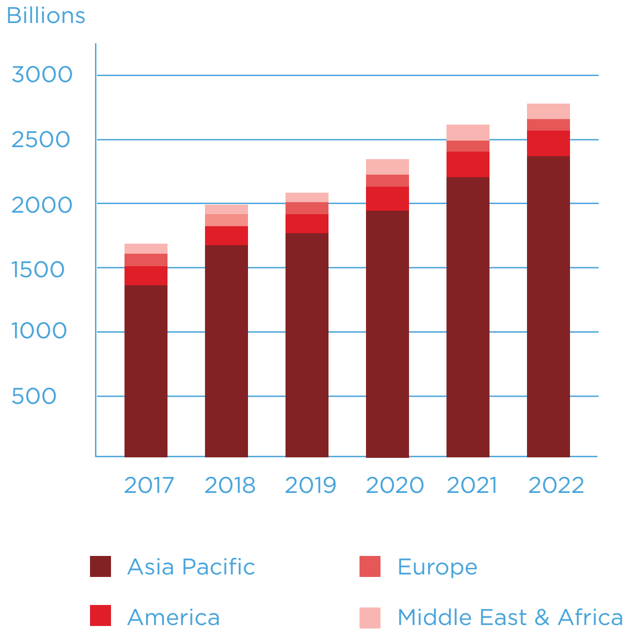
This platform used predominantly for social communication has the advantage of engaging its users. Such channels allow its users to share media and attachments thereby creating an interactive, user-friendly platform. The increasing acceptance of these channels for communication and boom of the digital age have laid the base for a more conversational and interactive commercial dialogue. Enterprises are set to use platforms such as RCS and OTT for an innovative and efficient way to communicate with their customers.

1.3 THE PROMINENCE OF COMMERCIAL COMMUNICATION- RISE OF A2P

SMS as a medium of commercial communication has been extremely well received. SMS is compatible with all mobile devices launched till date and is a preferred mode of communication for enterprises. A2P messaging enables pushing of bulk SMS to a predefined list of subscribers. These are generally unidirectional messages and are limited to commercial communication between enterprises and their customers for promotional and transactional communications. The architecture of such messaging enables enterprises to send messages from a software or web interface to their customer's devices through a mobile network connection. The growing use cases of A2P span the gamut of transactional and promotional objectives, with the former including appointment reminders, two-factor authentication, and text donations, and the latter including advertising and marketing, text-to-win, and mobile vouchers. Over the years, the scope of A2P messaging has broadened to engulf service messaging, along with the traditional transactional and promotional communications. Today, A2P messaging is a commonly used system leveraged for commercial communication to send personalised promotional campaigns, interactive services, bulk SMS and Customer Relationship Management (CRM) services.

Total global A2P SMS messages by region (2017-2022)

10

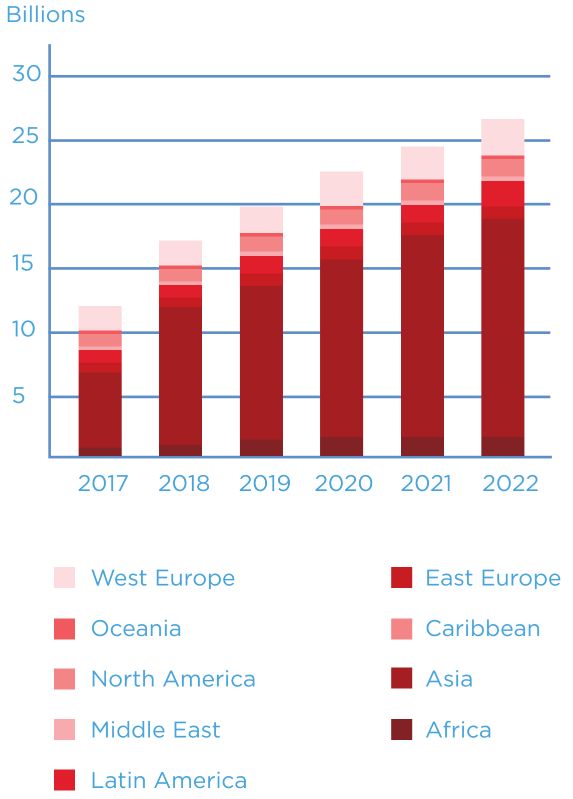


A2P messaging is based on how easily SMS can be integrated. Further, advancement in technology has made it possible for developers to build apps and send messages to users entirely through software. This functionality has helped a company like Uber to alert passengers that its driver is nearby. It is one of the core success of the A2P service.

> **The global A2P messaging volumes were over 1.7 trillion in 2017 and are expected to rise beyond 2.7 trillion by 2022. The A2P market is approximately worth $ 11.8 billion in 2017 and is expected to grow to $ 26.6 billion by 2022.**[11]

This rise in revenues and volumes of A2P ascertained the increasing importance and continued consumption of A2P channels for commercial communication. The growing availability and accessibility of Application Programming Interfaces (APIs), make it easier and less expensive for enterprises to integrate SMS into their existing customer-facing platforms. As per Mobilesquared research 2018, the A2P monetisation strategy is set to evolve from domestic and international A2P SMS, followed by phone number portability and verification information, Internet of Things, Machine to Machine (M2M) and lastly A2P messaging via operator-owned OTT apps. Buoyed by a mature commercial communication ecosystem, it is essential for the critical ecosystem players to work in harmony to sustain the growth of A2P messaging.

10 Global A2P Sms Revenues



1.4 KEY PLAYERS IN THE ECOSYSTEM

The global A2P messaging ecosystem is divided and governed by the presence of a large number of participants which includes enterprises, access providers, telemarketers, platform providers and developers, regulators and customers.

Over time, the players have become more interactive and have matured to co-exist and collaborate to bring innovation. It has resulted in creating more opportunities to increase the profit margins, hone their value proposition and increase customer engagement. As the customer experience landscape is of utmost importance, it is also important to deliver content tailored according to their preferences with their consent. Therefore, the relationship of the end-user with access providers and organisations is very delicate and significant.

Increasing use cases such as automated marketing, customer authentication and RCS across varied industries are driving growth in this front. Sectors such as Banking, Financial Services and Insurance (BFSI), Education, Real Estate and many more are actively reaping the benefits of A2P owing to its adaptability.

Aimed to serve the needs of their customers better, transactional and service messages were introduced. Such messages allowed the users to easily obtain details about the services or products they were purchasing or considering
to purchase.

01

Access Providers: They include basic telephone service providers, cellular mobile telephone service provider, unified access service provider, universal access service provider and virtual network operator (VNO). They contribute towards value creation by providing access to their customer base and offer their network services to A2P messaging platform and other players.

02

Telemarketers: The telemarketers act as gateways or intermediaries between companies and end users, and are responsible for collecting SMSs and other data to provide a centralised interface to users. They help enterprises from various industries such as retail, banking, e-commerce, etc. to deliver content seamlessly through multiple modes and reach their consumers. Thus, they play an important role in effectively distributing tailored content by filtering out unwanted information.

03

Platform providers and developers: The platform providers and developers design the APIs and libraries and ensure seamless integration of SMS, push notifications, email, etc. They are responsible for maintaining the velocity, adaptability and agility of the ecosystem in the age of disruption through digital technologies. They manage the network interconnections and ensure they are interoperable with access for all players while performing black- and whitelisting activities as specified by the operators. Considering the outreach of the A2P SMS market and big data, cloud computing is a preferred choice for deploying the robust architecture to minimize hosting and security concerns.

04

Enterprises: Benefits of commercial communication like ease of entry, adaptability, market reach and affordability have redesigned enterprises' market strategies to create an immediate impact on the lives of customers at a global level. It's several uses cases such as – promotional messages, appointment confirmations, product updates, bank transaction and authorization messages, allow enterprises to leverage this medium to easily connect with their target customers.

05

Regulators: Regulators ensure that all the players follow a code of conduct, follow best practices and maintain trust in the ecosystem. It is crucial for regulators to ensure that these communication channels are secure and transparent, commercially viable and protect consumers from fraud while delivering meaningful content with proper consent.

06

Customers: The customer is the end recipient of the intended commercial communication from an enterprise. The customer is responsible for setting his/ her preference and consent and communicating the same to their access providers. In this way, they have a strategic relationship with both the enterprise and operators.

“SMS based direct to consumer communication is one of the most effective channels for customer engagement for us at Future Group. We use this engaging channel to not only communicate promotional content but also leverage this medium to regularly update our loyal customers about their loyalty points balance, OTP for account validation etc.

Therefore, a secure and reliable messaging platform is at the very foundation of our customer-led retail business.

In this regard, TRAI’s recent regulation on Unsolicited Commercial Communication is undoubtedly a welcome step to curb spam messaging and potential fraud. We welcome this initiative and are optimistic about the positive impact this will bring to end-customers and businesses alike.”

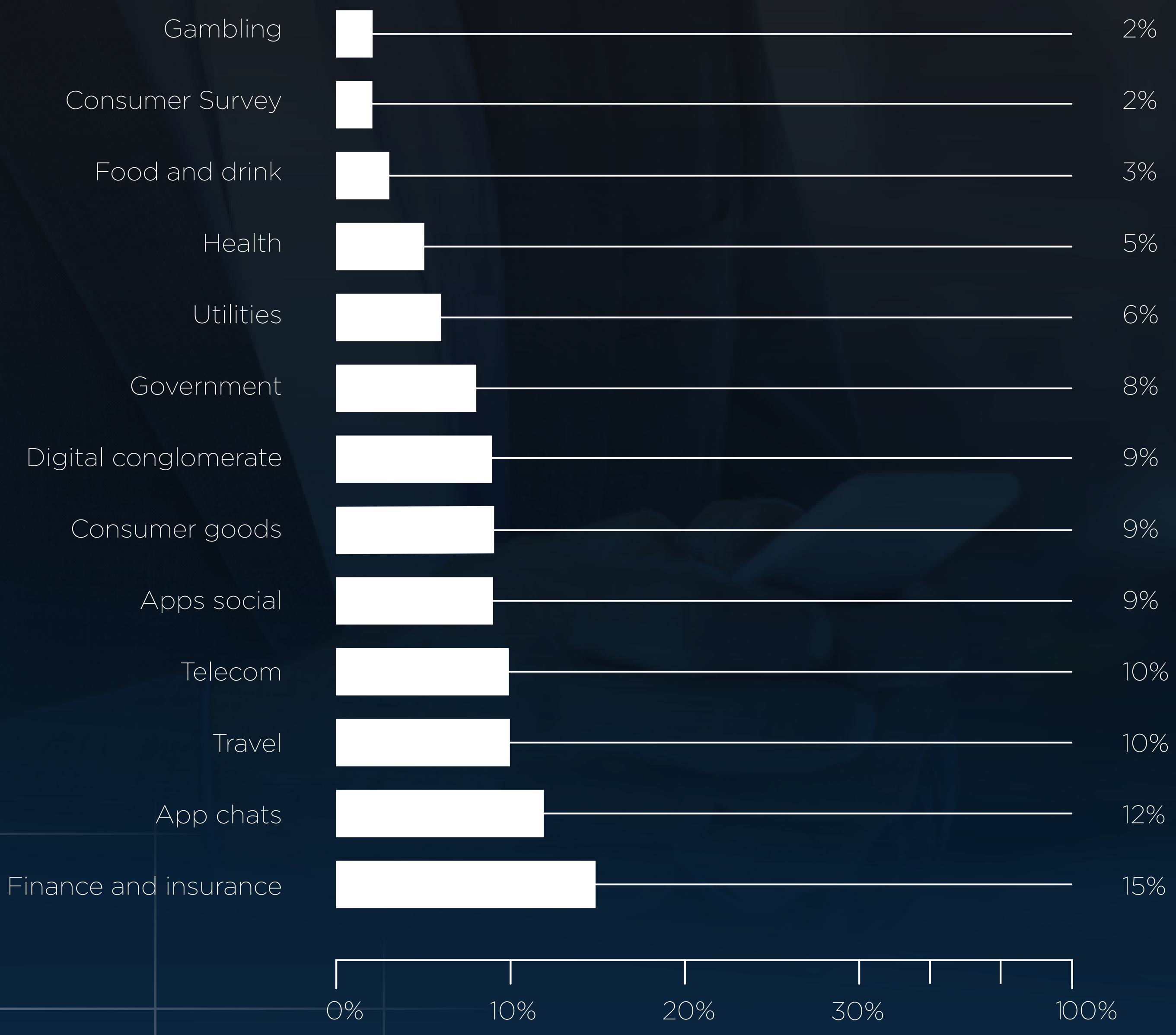
Rajat Mathur
Head Loyalty Future Group

SMS Coupons are 10 times more likely to be redeemed and sharedthan mail and newspaper coupons

22% of mobile coupons are shared with atleast 1 friend.

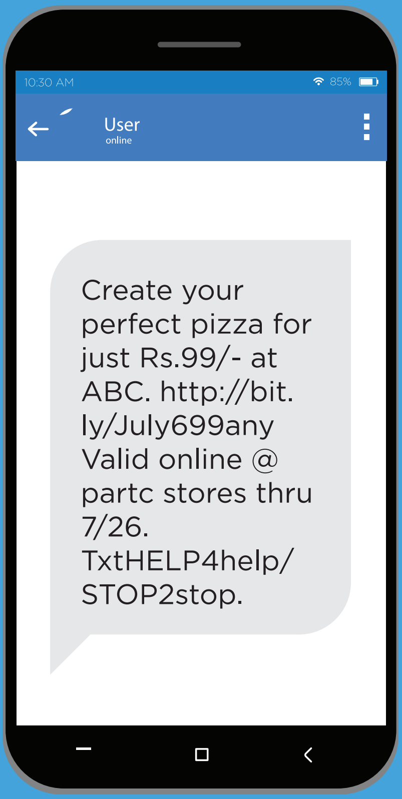
11

Total A2P traffic by sector

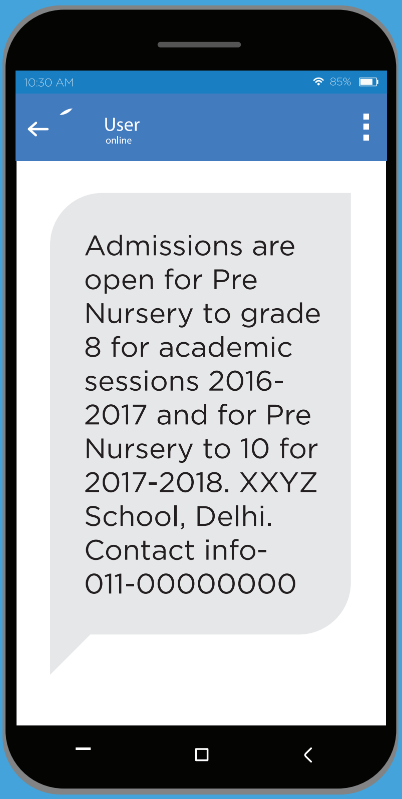


INNOVATIONAL USE CASES

Promotional messages

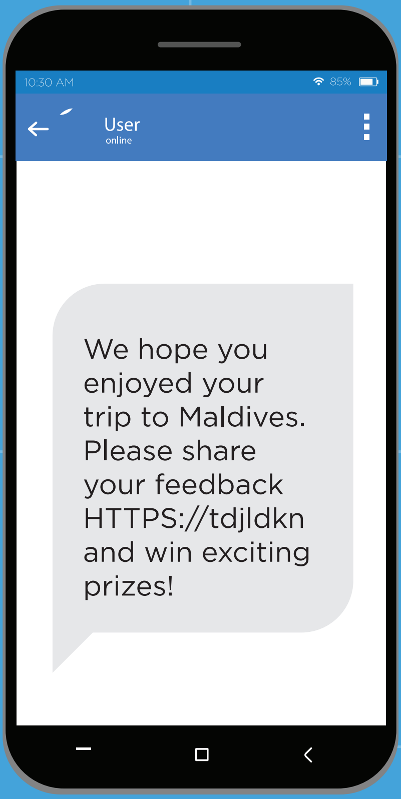


Create your perfect pizza for just Rs.99/- at ABC. http://bit.ly/July699any Valid online @ partc stores thru 7/26. TxtHELP4help/ STOP2stop.

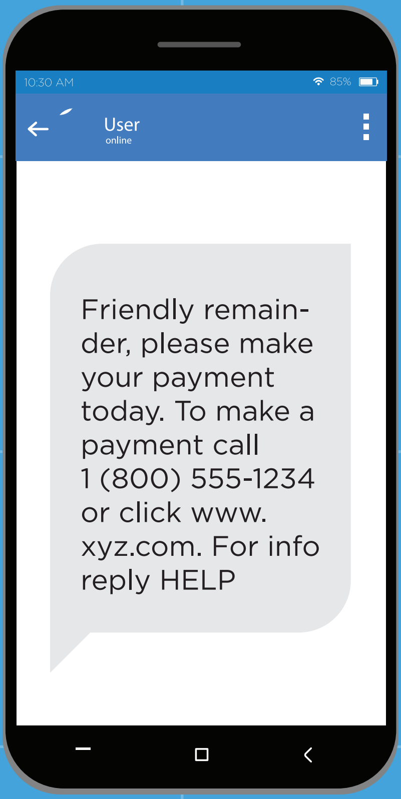


Admissions are open for Pre Nursery to grade 8 for academic sessions 2016-2017 and for Pre Nursery to 10 for 2017-2018. XXYZ School, Delhi. Contact info-011-00000000

Service messages

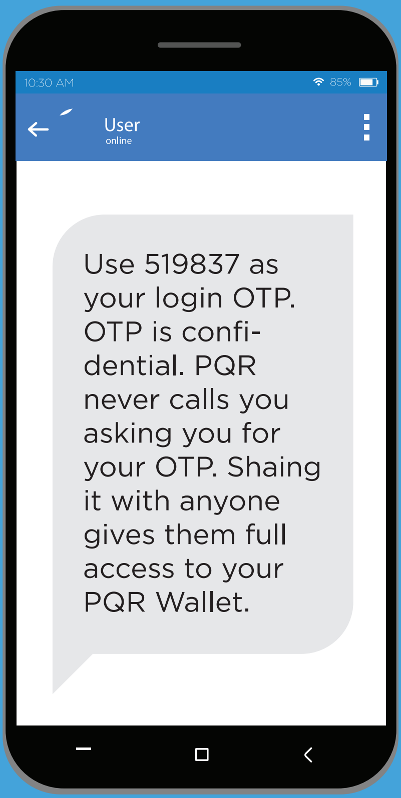


We hope you enjoyed your trip to Maldives. Please share your feedback HTTPS://tdjldkn and win exciting prizes!

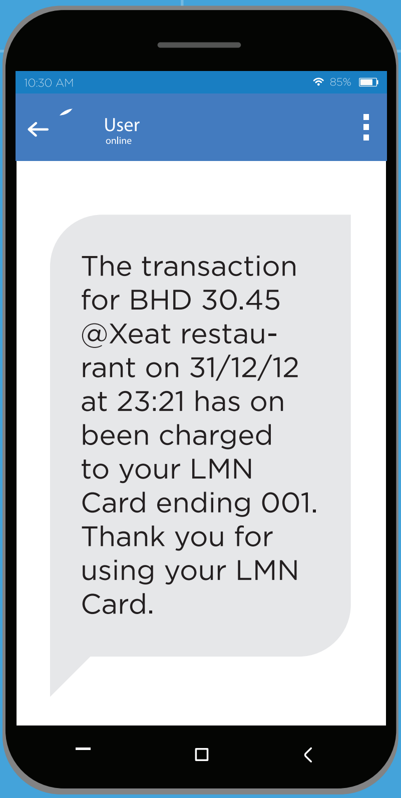


Friendly remainder, please make your payment today. To make a payment call 1 (800) 555-1234 or click www.xyz.com. For info reply HELP

Transactional messages



Use 519837 as your login OTP. OTP is confidential. PQR never calls you asking you for your OTP. Shaing it with anyone gives them full access to your PQR Wallet.



The transaction for BHD 30.45 @Xeat restaurant on 31/12/12 at 23:21 has on been charged to your LMN Card ending 001. Thank you for using your LMN Card.

2

OVERVIEW OF UCC

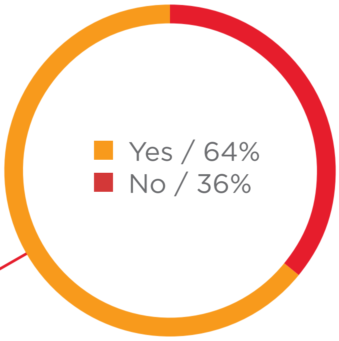
NIELSEN SURVEY RESULTS

COMPLAINTS ABOUT UNWANTED COMMUNICATION

Q8. Have you ever complained to your operator about unwanted calls or messages delivered?

About **2 in 3 people** have complained their mobile operator about unwanted calls/ messages

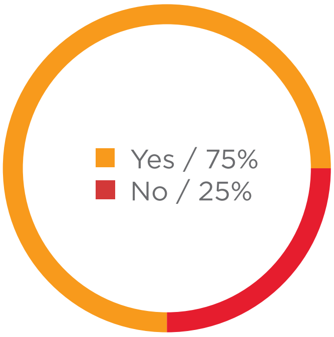
Amongst those who are not aware of ways in which they can register your choices and complaints, **55%** have never complained to their operator about unwanted calls/ message



AWARENESS ON HOW YOU CAN REGISTER YOUR CHOICES AND COMPLAINTS

Q9. Are you aware of the ways in which you can register your choices and complaints?

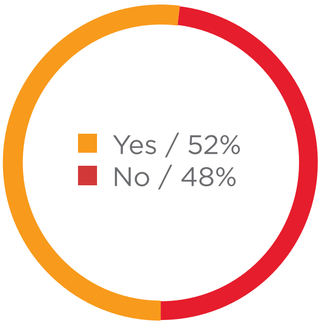
Awareness about how to register choices and complaints is high with **3 in 4 people** knowing how to do so



AWARENESS OF NEW REGULATIONS

Q10. Are your aware of the new regulation to curb Unsolicited Commercial Communication?

Less than half of the consumers are aware of the new regulation to curb Unsolicited Commercial Communication



OVERVIEW OF UCC

CCommercial communication has proven to be a definite boon for enterprises, telemarketers and telecom operators. However, there have been cases as well when the customer consents & preferences have not been honored, and their privacy is breached. A ny form of Commercial communication that is sent across to the customers without their consent. or is unaligned with customer preferences is termed as 'Unsolicited Commercial Communication' (UCC). Availability of affordable handsets, economical telecom services, the growing popularity of services such as A2P, ChatBots, etc. have a catalysing effect on the growth of UCC and have made it more rampant. UCC evolved from a cottage network of independent spammers into a highly sophisticated and technologically advanced industry but not in the most ethical of ways. Initially operating and keeping attacks at a smaller scale, spammers and fraudsters have matured in dodging the constantly evolving control environment. Today, UCC is a popular medium for committing various white-collar crimes such as credit card frauds, identity theft, bank frauds, data privacy breaches, etc. in addition to the routine spams.

2.2 TYPES OF UCC

Majority telemarketers and spammers use UCC to increase their sales or widen their market footprint by reaching out to a broad subscriber base at sub-optimal costs. Given the volume and the sensitivity of the information that enterprises have at their disposal, it has become incredibly lucrative for perpetrators to invade customer's space at any given time.

> **Mobile Network Operators (MNOs) have conservatively estimated that close to 10% of A2P revenues are lost to frauds which are approximately $ 1.5 billion in a year of over $ 16 billion A2P Market. Perpetrators have identified numerous ways of dodging the existing controls landscape and have been successfully bypassing systems, networks, firewalls, etc.** **successfully bypassing systems, networks, firewalls, etc.**[12]

Over 1.7 trillion A2P SMS were sent to customers in 2017, of which approximately 15% were two-factor authentication SMSs, i.e. nearly 300 billion SMS with authentication codes that could be potentially intercepted by rogue companies or individuals.

Majorly, UCC can be categorised into the following three genres:[12]

01 Invading Customer Space

- Spam and Fraud Calls
- Robo and Silent Calls

02 Breaching Data Privacy

- Phishing or SMSishing
- Spoofing

03 Scamming the ecosystem

- Botnets
- SMS Grey Routes
- SIM boxes / SIM farms
- Malware Attacks

2.2.1 Invading Customer Space

Almost all industries today are customer-centric, and thus while enterprises themselves, it is essential to ensure customer's convenience while honouring their personal space and consent. In an attempt to reach out to a broader user base, certain unscrupulous enterprises and telemarketers have carved numerous ways to reach to the target audience irrespective of the audience's preferences and concerns.

» **Spam and Fraud Calls**

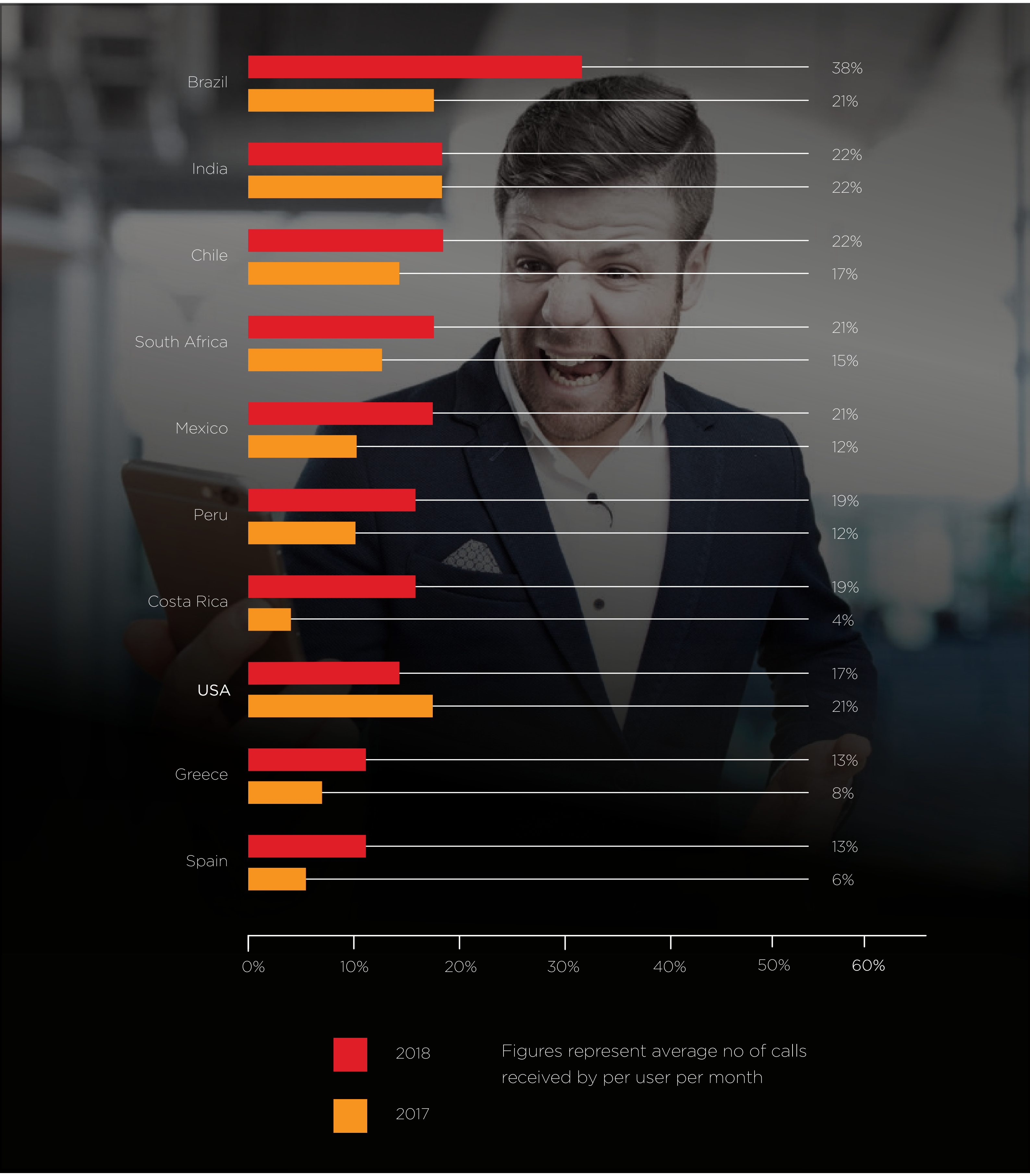
Communications Spam and scam communications by telemarketers have become a growing menace. Telemarketers are connecting with consumers at any nick of time without their consent and preference. These include cold calls from call centres promoting goods and services which often lead to customers sharing information that can be used for their own monetary disadvantage. It allows spammers to gain their financial and personal information to earn monetary benefits and thus, scam calls can cause serious financial implications to the subscribers.

> **Around the world, spam calls increased by 300 per cent as per a Truecaller 2018 report. India is placed second in the top league of countries where mobile subscribers have been affected by spam and cold calls.[13]**

The increasing number of unsolicited and unscrupulous messages flooding customer inboxes, often result in the loss of relevant information as it may get buried under hundreds of unwanted messages a customer receives daily. Since the customers overlook most of these messages the entire purpose of CC both from customers and enterprises' perspective get defeated. Neither does the customer get awareness of the enterprise and its products nor does the enterprise effectively capitalise on the economies of scale of sending bulk SMS as the conversion rate becomes very low leading to additional costs.

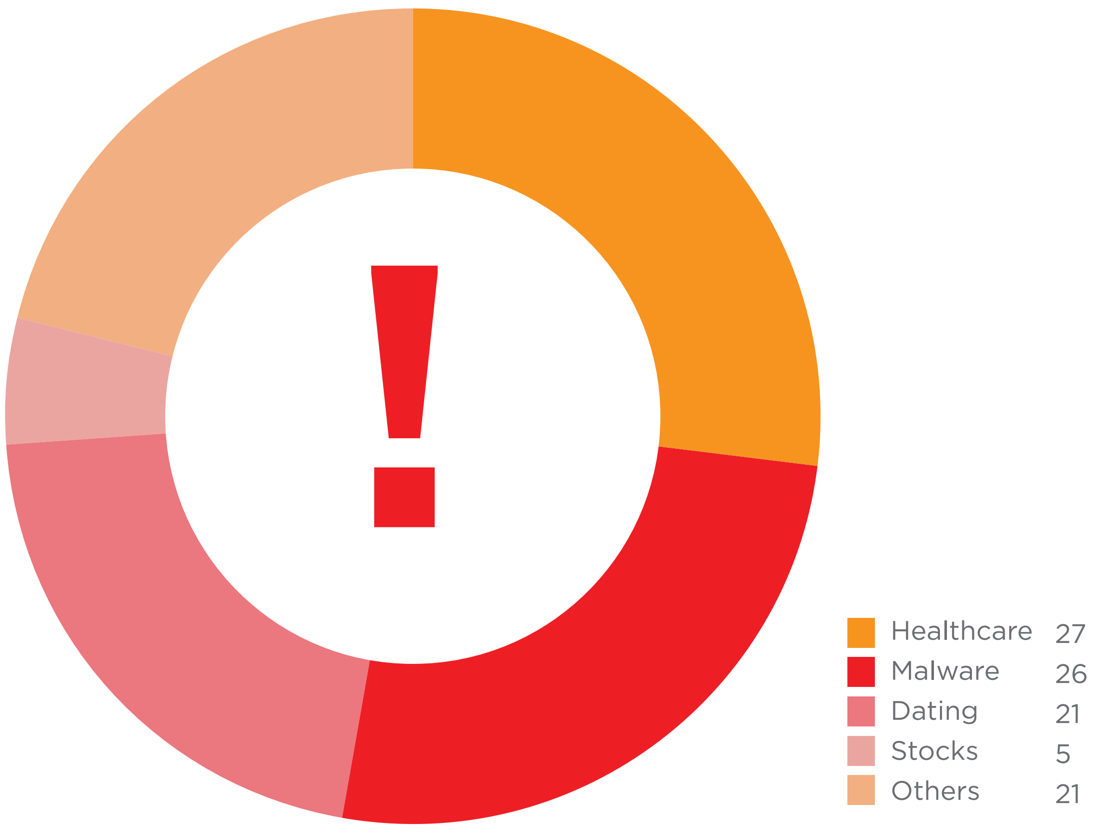
13

Top countries affected by SPAM calls in 2018

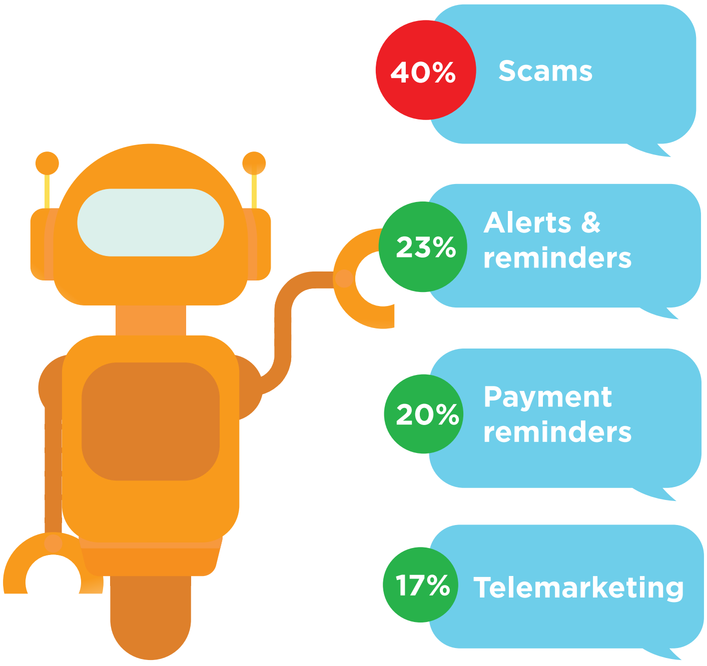


Figures represent average no of calls received by per user per month

14 Most prevalent spam content categories worldwide in 2017



15 Robocalls by categories



» **Robo and Silent Calls**

Robocalls are automated phone calls which contain a recorded message, primarily used to promote goods, services, charities or donations. Similar calls but when the mobile user receives a call, and nobody answers from the other end. Such requests are called silent calls and are often the first step to target customers to stimulate fraud and theft. The sudden spike in robocalls can be contributed to easy access to the internet and low cost involved in using autodialers and VoIP to make thousands of call every minute.

In the United States of America, as of December 2018, 4.7 billion robocalls were placed, 40% of which were identified as spam.[15]

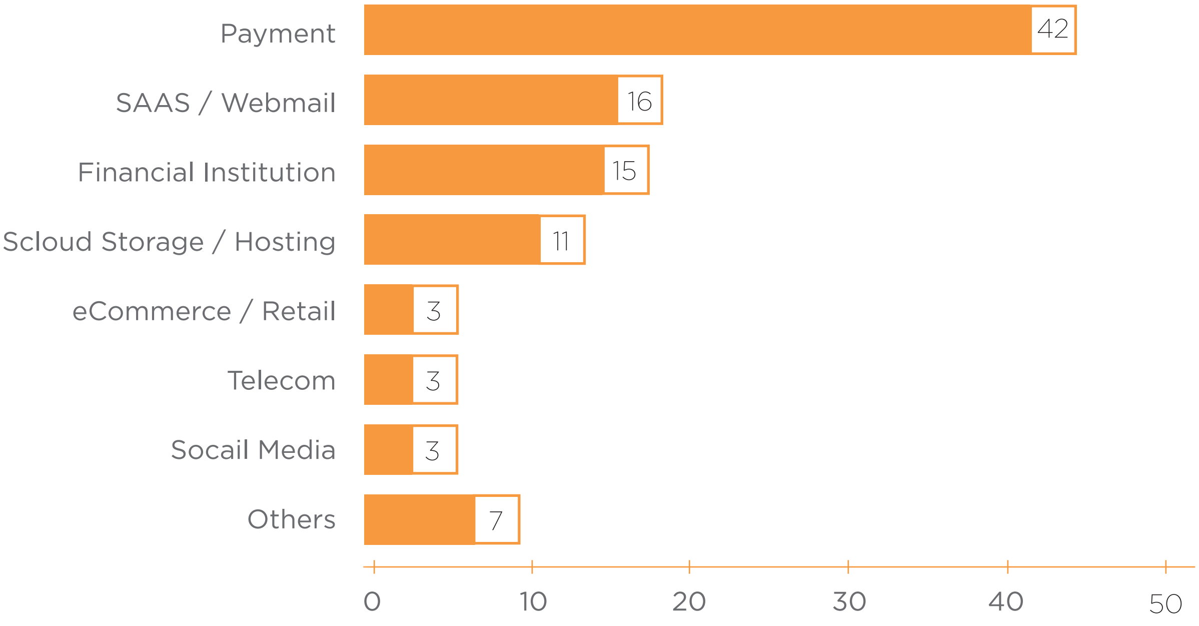
2.2.2 Breaching Data Privacy

With the emergence of the multi-billion data-brokerage industry, massive volumes of confidential customer information such as bank details, phone numbers, addresses, etc. are sold to spammers and scammers at unbelievably low prices. Even though data privacy and data security are interchangeably used, they are two distinct terms - Data privacy refers to data management right from the way how data is collected, shared and utilised whereas; data security, as the name suggests relates to protecting data from malicious and phishing attacks.

» **Phishing or SMSishing**

Phishing is when attempts are being made to establish communications with the customers by disguising the sender as a more trustworthy organisation purely with the intent of gaining customer's attention and trust. Subsequently, the customer is allured into sharing their personal or banking information with the sender either by using links to an original looking fake website, hacking actual logos, etc. Social engineering has evolved with time, and the underlying approach has become more targeted than ever. Fraudsters are now deploying more sophisticated tactics such as modifying the subject line of emails, etc. to make it look more legitimate and authentic enough to dupe customers easily. Additionally, exploitation of customers through their emotional impulses and luring them to pay in cases of natural disasters, sickness, charities etc. are becoming common forms of phishing.

16 Most-Targeted Industry Sectors for Phishing attempts , Q4 2017 .



In 2017, the new phishing attack was identified which aimed at stealing usernames and passwords of Gmail and other linked services and successfully effected around 1 billion users worldwide. A Gmail sign-in form was shared which looked exactly like the typical and legitimate sign-in page. However, the URL was changed, which gave the hackers full and free access to user accounts. Another case came to light where a emails mail that appeared as ones from Netflix were circulated requesting users to update their credit card details.

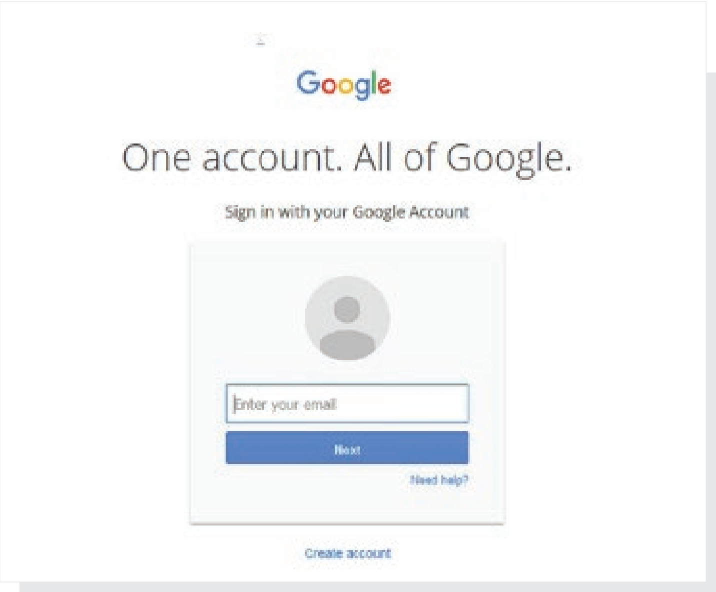
» **Spoofing**

Spoofing is a means of delivery that fraudsters have adopted to spread malicious content to users phones, laptops, tablets, etc. Aesthetically similar to phishing, spoofing too uses similar disguise technique wherein the actual name of the sender, subject line of an SMS/email, etc. is replaced by a more trustworthy and authentic looking source to allure the customer enough to follow instructions in the SMS/email. The communication predominantly includes a link that the customer would be ill-advised to click which in most cases would download malicious files or malware on to the customer's device, compromising system security. Such illegal activities as ransomware, CEO fraud, Business Email Compromise (BEC) inflict a heavy toll on small, medium or big enterprises.

'Neighbourhood Spoofing', an updated variant of ID Spoofing allows scammers to place calls from phone numbers that appear to be generated from within the surrounding area of the recipient thereby increasing the probability of the calls getting answered. They are also tapping demographically based weaknesses of users, to allure them with lucrative deals or promotions such as weight loss, astrology, lottery, phone giveaways etc. .

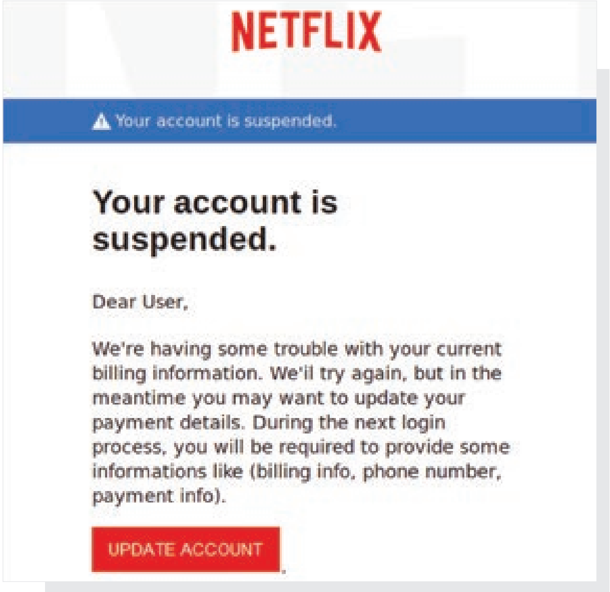
"SPAM is a big nuisance. All of us get dozens of unsolicited calls and SMS daily! Now with TRAI's new regulation SPAM will be a thing of past. Added to that message will become more secure which is great news for the banking industry which sends a lot of confidential communications to our customers over SMS."

- Vivek Kumar Singh
Chief Manager-IT Allahabad Bank



One account. All of Google.

Sign in with your Google Account



⚠ Your account is suspended.

Your account is suspended.

Dear User,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details. During the next login process, you will be required to provide some informations like (billing info, phone number, payment info).

2.2.3 Scamming the ecosystem

Telecommunications is the underlying services to commercial communications. Being a dynamic industry in itself, telecom undergoes technological and architectural transformations on a very regular basis. While these transformations are necessary for improving the quality and expanse of services, it is also pertinent to upgrade the control landscapes as well. Perpetrators have evolved over the years and have carved out numerous technologically advanced ways of scamming the not-so-upgraded controls architecture thereby magnifying the effects of UCC.

» Botnets

Botnet is a network of private computers or Internet-connected devices infected with malware and malicious software to generate spam and are controlled without the User's knowledge. They are used to launch Distributed Denial of Service (DDoS) attacks and ransomware attacks giving perpetrators access to a plethora of user information, information which is mostly used for fraud. The botnets are present all around the world, but Russia, Brazil, China, India and Vietnam have been identified as significant hotspots. IP blacklisting was considered a breakthrough where illegal and dark-web IP addresses were added in the blacklist to block the traffic generated through them. However, due to its static nature, it found limited success. In another attempt, recently, the 'CAPTCHA' method was introduced to identify bots from humans using fuzzy tests.

17 Grey route detection

Firewall deployment 83% by 2022 48% of mobile operations in 2017

Grey-route traffic from 799.4 bin in 2017 to 418.9 bin in 2022

A2P SMS sent 1.7 tln in 2017 46bln per day 2.8 tln in 2022 77bln per day

Revenue Leakage $5.8 mln in 2018 $3.9bln in 2022 between 2017-2022

» SMS Grey Routes

A grey route is an A2P SMS delivery path where the sender (for example, a low-cost aggregator) does not have a commercially binding termination agreement with the ultimate receiver (the network operator) and consequently does not pay the operator what it is owed for terminating the traffic. Grey routes are often conduits for spam and other types of unwelcome SMS communications. The absence of IUC agreements among operators allowed spammers to send bulk messages to consumers and generate a large amount of traffic at bare minimum costs. As a result, access providers across the globe are losing significant potential revenue to such fraudulent messages.

> **The development of Signaling System 7 (SS7) in 1993 enabled international P2P traffic and allowed subscribers around the world to interact with one another using SMS. For every SMS, the terminating network operator would charge a certain amount to the originating network operating.**

Since P2P messaging is majorly a back-and-forth communication, the payment system was phased out as the charges levied almost used to get nullified. A2P messaging aggregators were quick to identify network vulnerabilities here, hack into the network and send bulk SMS to customer using this network. The terminating network provider considered the incoming SMS to be regular P2P messages and therefore these messages went ignored consistently. In 2017 itself, $ 8 billion was the total loss of potential revenue for network operators from SMS grey route frauds.

Over the years, network operators have adopted numerous measures and have been able to reduce the number of fraud instances through grey routes successfully. The total grey-traffic is also speculated to decrease from 799 billion in 2017 to 418.9 billion in 2020. However, the threat from unethical uses of grey routes is imminent as it still accounts for 47.7 per cent of the entire A2P SMS traffic network. [17]

» SIM boxes/ SIM farms

SIM box, also known as SIM bank, GSM gateway or SIM farm is a method that exploits the messaging tariffs aimed at consumers. It is defined as a device which essentially is a bank of SIM cards linked to a computer. Spammers utilise SIM boxes to circumvent international voice tariffs and take advantage of an operator's network to send a massive volume of promotional spam and nuisance texts to consumers without their consent.

> **As technology is becoming more sophisticated along with decreasing SMS rates, it has become more difficult for MNOs to detect and block such spam texts.**

Also, SIM banks are finding their space in mobile devices and further manipulate location-based detection and blocking mechanisms of the device. IMEI reconfiguration has made it all the more difficult to trace the traffic generated through SIM boxes.

Considered as a significant threat, SIM box fraud costs the telecom industry around $3 billion in revenue per year. Recently in India, some intelligence was recovered from a J&K, based MI branded device which led to busting of eight illegal VoIP (voice over internet protocol) exchanges in Hyderabad that were reportedly being used by Pakistan intelligence agencies for espionage operations in India. The Telangana police recovered around more than 30 sim boxes and more than 65 billion sim cards along with the arrest of four individuals suspected of promoting terrorism.[18]

» Malware Attacks

Malware attacks are sending out messages which include links, which if clicked by the recipient, would install viruses and Trojans on to the user's device. This allows fraudsters and hackers to gain control of the user's device and perform various actions like send texts or make calls without authorization, secretly monitor user's behaviour, read banking and other personal messages, etc.

Cybercriminals have incorporated machine learning techniques to design new pieces of malware which are getting aggressive with time. Mobile security firms are identifying such malware apps daily to limit the impact. However, fraudsters use the complex distributed network to strengthen attacks, thereby making it harder to detect the primary source of the threat. In 2017, Google shelved 50 apps from its App Store as they were infected by a type of mobile malware known as 'ExpensiveWall'.

> **It was downloaded around 5.9 to 21.1 million times and used an advanced obfuscation technique 'packed' which compressed malicious programs and encrypted them to avoid detection. In less than 4 days, ExpensiveWall had infected over 5000 android devices.[19]**

In May 2017, another malware named 'Judy' was installed 36 million times and was identified in 40 apps . Similarly, in four other instances, Google removed another 136 apps that were infected with similar malware. It is imperative to note that researchers have not been able to quantify the monetary impact these attacks.

2.3 CASE STUDIES

2.3.1 UnityPoint Health and NHS Data Breach

Around 1.4 million patient records were exposed in the aftermath of a phishing attack at UnityPoint Health's system. Confidential information related to patients and employees like Social Security numbers, dates of birth, diagnoses, prescriptions and even payment information was leaked. A similar kind of breach happened at NHS where sensitive data about 150,000 patients was leaked due to a coding error on their platform.[20]

2.3.2 Fake Bank Apps and Links

Tricking consumers into downloading spoof apps of major banks like Citibank, Well Fargo, Santander, HSBC etc. has become the most popular trick up fraudsters' sleeves. These banks have become lucrative targets in the cybercriminal space owing to their massive customer base. According to a survey conducted by Avast, one in every three customers ends up downloading counterfeit apps instead of the official Bank apps. This serves as a gateway for scammers to install malicious content or malware on the phone, hence illegally gaining access to personal information like username, password, bank details etc.[21]

Similarly, a lot of scammers mask the header of the message and share malicious links to get insights into the customer's personal information. Recently in India, fraudsters circulated a lot of hoax emails and messages using RBI and SEBI's signature within users which required them to fill in their bank details to win a lottery. Given that it's challenging for conventional end-users to spot the differences, many such customers have fallen prey to such schemes and have become victims of financial fraud through SMS phishing and spoofing .

2.3.3 Fake Website and misleading advertisement

Recently, the internet world and the newfound trend of 'online shopping' has become a convenience in India and around the world, also leading to an increase in the threat of fraud and data theft. According to a report, 'Digital Consumer Insights 2018' released by Experian, one in every four customers is a victim of online fraud, and around 24 per cent have directly experienced fraud during online transactions. India has been considered the most tolerant country in the APAC region towards fraud through services like – 57 per cent in telcos, 54 per cent in banks, and 46 per cent in retailers. The report also highlighted insights like

» 50% said they are most comfortable sharing data with banks
» 30% are uncomfortable sharing data with branded retailers
» 51% will share personal data to avail of service offerings[22]

A leading consumer goods company in India, Patanjali, paid a financial penalty of Rs 11 lakh on the grounds of misleading and misrepresentation of its products.[23] Cashing on its market presence, cybercriminals also duped investors by alleging partnership and distribution of goods worth Rs 10 lakh through fake websites and promotional links through SMS. On the pretext of proposing dealership, such fraudsters used fake URL, i.e. www.patanjalidistributors.org, SMS links and scam calls to contact dealers and hence, robbing them of their money. Similarly, another such case came into the light where customers got SMS links with promotional and discount offers related to PepperFry. Such links led them to fraudulent and phishing platforms where they would be trapped in the almost genuineness of the fake sites. The customers trying to avail such offers ended up losing money, falling prey to such phishing messages.

2.3.4 Call Centre Scam in the US

Around five India-based call centres based in Ahmedabad in collaboration with 15 people, ran a multimillion-dollar fraud which affected around 2,000 US citizens and led to financial losses worth $ 5.5 million. Massive volumes of calls were made through these call centres frequently impersonating themselves as officials from Internal Revenue Services (IRS) or US Citizenship and Immigration Services (USCIS); luring the customers to fall in the trap of – payday loans. The perpetrators ran an elaborate fraud and money laundering scheme of threatening the customers, mainly elderly and legally migrated citizens with imprisonment, deportations or arrest failing to submit their taxes. Leveraging the ever-growing data-brokerage industry, these scammers gained personal information and started calling the potential victims. Once the victims were ready to pay, the money was moved and liquidated around through wire-transfers and purchasing prepaid debit cards. The US court has ordered a jail term of approximately 20 years along with deportation for the fraudsters involved in this scandal, making it one of the most significant cases of arrest and sentencing of Indian cases or people of Indian descent in the US history.[24]

On the same concept, several fraud calls were also made to customers in the Indian terrain, threatening them on consumer court-related matters. The spammers would collect information like name, date of birth and other such details and also offer to save them by asking them to pay a certain amount. Such scams are very popular with immigrants living in foreign countries, and they are often considered as 'easy preys' as they risk deportation and getting caught in the complexities of the legal system.

> **Numerous call centres in Delhi were also found targeting customers by circulating pop-up messages related to malware installed on their networks. Such callers disguised themselves as customer care executives from Microsoft, offered customers support by charging them a fee of $ 100- 500.[25]**

During the investigation conducted by cybercrime cell, cheques in the name of Microsoft Tech Support, call recordings, virtual/automatic dialers, audit trails for call logs, conversations, payment gateways and servers containing personal information related to customers were uncovered.

2.3.5 One Ring Scam

Lately, 'One Ring Scam' has allegedly become a common occurrence, leading to data theft and monetary losses. The scammers conned the common public by using automatic dialers to call random numbers and leaving a missed call or a dodgy text asking them to call back urgently. Upon returning those calls, the users are usually directed towards international hotlines – majorly an adult site or premium numbers, thereby debiting money from user's prepaid balance along with the risk of losing personal information.

> **To prevent this, DoT also tried to raise awareness among the general masses warning them not to pick calls from extensions like +216, +92 and +375. Upon complaints from several users, it was noted that a group of fraudsters in Africa were trying to get access to phone and personal data through such fake calls.**[26]

Through the enhancement and innovation of communication platforms with respect to use cases and technology, A2P messaging will remain an essential source of revenue for operators and enterprises alike. The growing popularity of the A2P channel reflects a classic example of a 'low margin high volume' revenue model. Though this model boasts of a wide scale of benefits, it also invariably creates a broader scope for fraud. The lack of barriers of entry are leading to an exponential increase in spam calls and messages and spread of fraudulent activities leading to financial losses. Such nuisances ultimately affect the users' experience and trust in the ecosystem. Business models of such nature warrant for implementation of robust regulatory frameworks to control the mounting problems of UCC.

> **"As a diversified company with presence in sectors such as housing finance, real estate & wealth management, we have a robust multi-channel customer communication strategy. SMS is one such channel that we use quite effectively to relay critical information to our customers such as OTP, details on loans and investments etc.**
> **Being strong advocates of customer privacy, we welcome TRAI's new regulation aimed at curbing spam and promoting branded communications which will help in building trust with our customers."**
>
> - Vivek Attavar

3

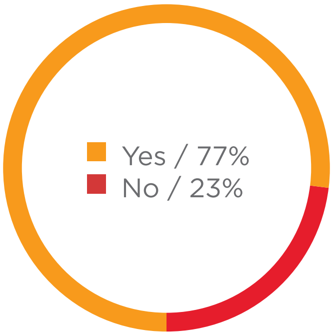
REGULATORY LANDSCAPE ACROSS THE GLOBE

NIELSEN SURVEY RESULTS

PUSH NOTIFICATIONS ARE ANNOYING

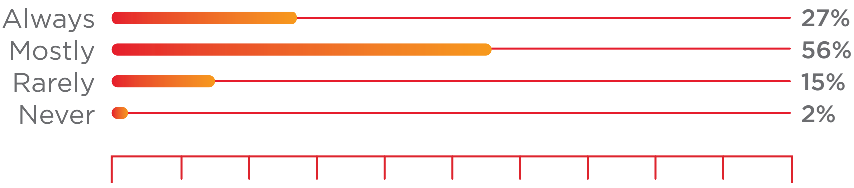
Q11. Do you feel the push notifications from your installed apps are equally annoying as the unwanted messages or calls?

More than **3 in 4** consumers find push notifications annoying



RECOGNIZING THE SENDER OR BRAND FROM THE MESSAGE HEADER

Q12. How often do you recognize the sender or brand from the message header?



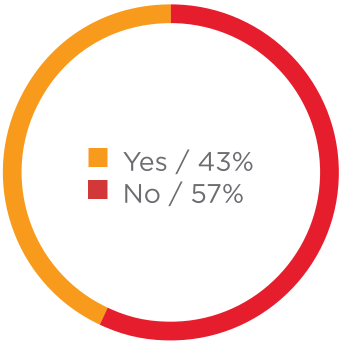
Only about 5 in 10 say they can mostly identify the brand from the message header

Consumers in metros are more likely to identify while consumers above 45 years say rarely identify the brand

VICTIM OF FRAUD DUE TO EMAIL, SMS OR CALL

Q13. Have you ever been a victim of fraud due to Email, SMS or Call on Ponzi schemes, lottery, and requests on sharing the OTP or CVV number, etc.?

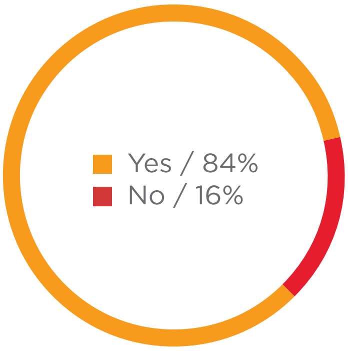
About **4 in 10** consumers have been a victim of fraud



TRUST IN YOUR BANK

Q14. Do you think the communications from your bank e.g. OTPs, balance updates, transaction messages (debit/ credit), etc. are secured?

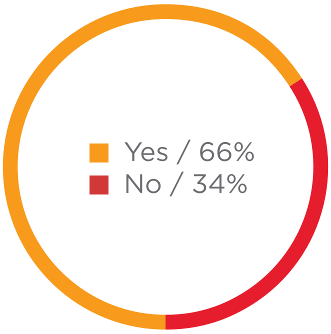
Majority of consumers believe their **communication from their banks are secured**



TRUST IN MOBILE OPERATORS

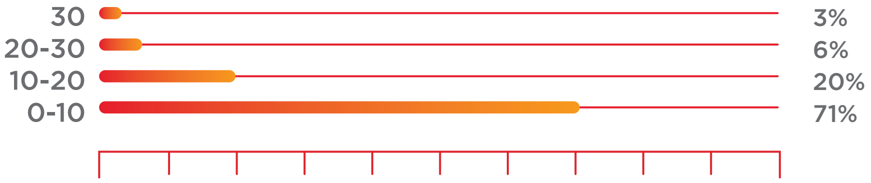
Q15. I Do you trust your mobile operators with regards to data privacy and controlling unwanted communication?

2/3rd of consumers trust their mobile operators with regards to data privacy and controlling unwanted communication



UNWANTED CALLS AND MESSAGES RECEIVED DAILY

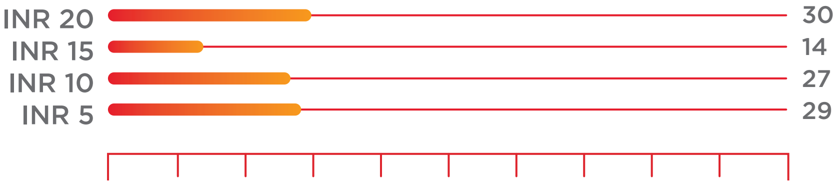
Q16. How many unwanted calls and messages do you get in a day?



On an average consumers receive **up to 9 unwanted messages or calls daily** – slightly higher among females (~10 unwanted messages or calls)

HOW MUCH CAN CONSUMERS PAY TO SECURE THEIR DATA

Q17. If given an assurance of data privacy and security, what is the amount that you would happily pay per month?



Young and tier 2 consumers are not willing to pay more than **5 INR to secure their data**

Middle aged consumers seem to be willing to pay as much as **20 INR per month to secure their data**

REGULATORY LANDSCAPE ACROSS THE GLOBE

Voluminous, pervasive and volatile are some of the most prominent characteristics of Commercial Communication. The expanse of commercial communication is such that it can reach customers at any time, which if not ethically used, would lead to customer dissatisfaction. While on one hand, businesses are making the most of commercial communication to expand their customer base and move geographies, customers' preferences, consent and privacy cannot be compromised. Regulators across the globe have time and again introduced or strengthened mandates to ensure that enterprises while pursuing their commercial interests, do not hamper customer space. Customers and their best interests are at the forefront of all regulatory initiatives.

At its core, the significance of having a resilient regulation is to clean the commercial communication ecosystem and ensure customer convenience. Commonly, regulators across the globe are making efforts to ensure the following –

» Obtaining customers consents/ opt in's
» Registration of senders to establish trust in the ecosystem
» The importance of giving consumers an opt-out option with details on how to unsubscribe from the particular form of commercial communication.

However, the innovation in technologies, has given a free reign to individuals, telemarketers and enterprises to spam customers, and adopt fraudulent activities with ease. The increasing rate at which such cases are advancing and technology is evolving, has surpassed the regulatory controls worldwide.

> **Though regulators have been increasingly focusing on tailoring their regulations to suit the changing requirements of consumers, they have resulted in only a marginal and not a substantial decrease in the disruption caused by unwanted commercial communications.**

South Africa : Protection of Personal Information Act, the Consumer Protection Act, and the Electronic Communications and Transactions Act[27]

Regulatory Authority - Internet Service Providers' Association (ISPA)

Key Features:
» Consent through opt-in model
» Unsubscribe option to users
» Clear marketing content with proper headers and contact information.

Penalties:
» No maximum threshold along with imprisonment for a period of maximum 12 months.

Canada : Canadian Anti-Spam Law (CASL) 2014[28]

Regulatory Authority - Canadian Radio-television and Telecommunications Commission ("CRTC")

Key Features:
» Organisations to operate on 'Opt-In' model
» Unsubscribe option to users with processing time of 10 business days
» Identity and contact information of sender to be mentioned clearly
» Right of action - Provision of filling lawsuits

Penalties:
» Fines upto CA$1 million for individuals
» Fines upto CA$10 million for organisations

USA: CAN-SPAM Act, 2003[29]

Regulatory Authority - Federal Trade Commission (FTC)

Key Features:
» Organisations can send messages to anyone if they comply with content
» Unsubscribe option to users with processing time of 10 days
» Clear marketing content with proper headers and contact information.
» Follows Opt-out approach

Penalties:
» Fines of up to USD 16 000 per violation per individual email.

UK : Privacy and Electronic Communication Regulations in 2003 (ePrivacy Regs) or (PECR)[30]

Regulatory Authority – Ofcom (Voice calls) and ICO (Electronic communication)

Key Features:
» Consent through opt-in model
» Unsubscribe option to users with processing time of 28 business days
» Clear marketing content with proper headers and contact information.

Penalties:
» Director liability with penalty amount upto GBP500, 000 including criminal prosecution, non-criminal enforcement and audit

China : Measures for the Administration of Internet Email Services, 2006 and the Consumer Rights Protection Law, 2013[31]

Regulatory Authority – Ministry of Information Industries (MII)

Key Features:

- Opt-in approach along with proper certification
- The word 'ad' should be mentioned clearly in the subject stating the commercial nature
- No cloaking or masking of sender's identity
- Unsubscribe/ opt out option to users with processing time of 30 business days
- Contact information of sender to be mentioned clearly
- No blacklist keywords should be present in any emails or texts

Penalties:

- Heavy fines can be levied ranging from CNY 10,000 to CNY 30,000 per individual email

Australia : SPAM Act, 2003[32]

Regulatory Authority - Australian Communication and Media Authority (ACMA)
Accompanied by Spam Regulations, 2004 and Telecommunications Act, 1997

Key Features:

- Any organisation sending communication will fulfil three requirements:
- Consent through opt-in model
- Unsubscribe option to users with processing time of 5 business days
- Identity and contact information of sender to be mentioned clearly

Penalties:

- Fines ranging from AU$1.7- 2.1 million in case of violations

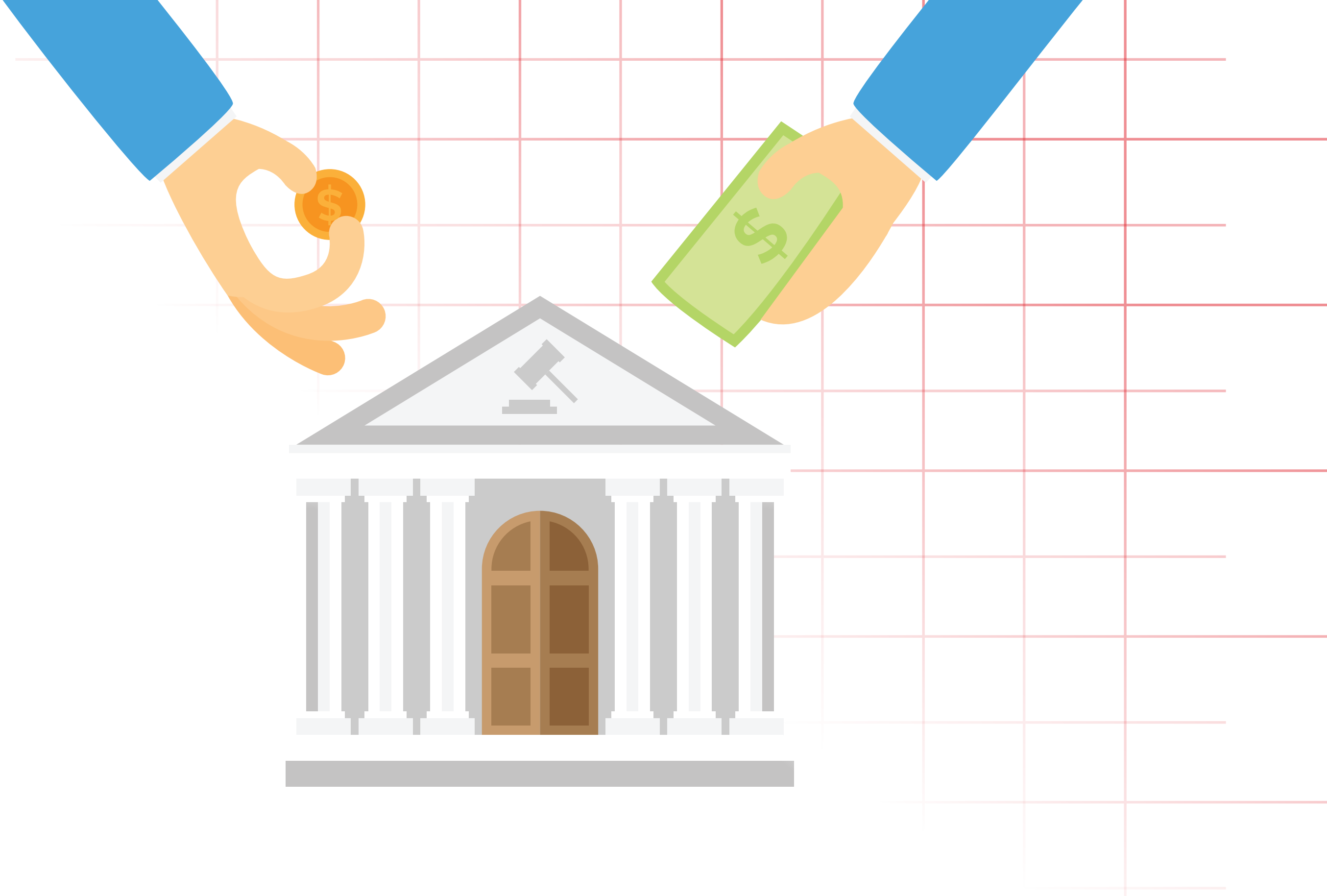
EU : GDPR and e-Privacy Regulation[33]

Key Features:

- Any organisation sending communication will fulfil three requirements: positive opt-in, i.e., eliminating pre-ticked boxes and also forces organisations to be very granular while asking for consent
- Cross-border data transfers with approved 'certification schemes'
- Codes of conduct like entering into proper MoU or agreements with a third party
- Mandatory encryption of communication

Penalties:

Financial penalties upto €20 million



3.1 GLOBAL REGULATORY LANDSCAPE

Regulations today, are slowly embracing the need for double opt-in or a form of two-step authentication. This would require recording of customers consents and ensuring a confirmation from them for the same. This is increasingly being enabled through SMS authentications in the form of one time passwords (OTP) for customers to confirm and validate their consents and preferences.

> **In Australia and Germany, double opt-ins are a mandatory requirement. German courts, on numerous occasions have also held that a single opt-in process is not sufficient proof of prior consent.**

Another good practice in some countries and a regulatory mandate in others requires message templates to carry clear information of the mode to opt-out/unsubscribe from receiving further communications. In counties that need registration of opt-in and opt out, the same is updated over a span of a few days and not on a real-time basis.

In **Canada**, under the CASL, senders must honour submitted opt-outs within a span of 10 days of the request thereby allowing enterprises to continue messaging customers until the opt-out request has been implemented.

Today, many governments and regulatory bodies are upgrading their regulatory frameworks, policies and governance models to safeguard the commercial communication ecosystem. Though regulators across the world are actively involved in creating strong control measures to curb UCC, they have to be equipped with similar or more superior technologies to combat the violators.

Determined to create a trustworthy and a secure environment and to enrich user experience, regulators are blending their mandates with advanced technological solutions, collaboratively known as Regulatory Technology or RegTECH. India is one of the few countries that have successfully implemented the integration of a superior technology such as blockchain within its regulatory landscape.

Australia[32]

Several cases have come forward in 2018 where ACMA has taken strict actions against organisations who have breached the Spam Act

» November—Foxtel Management Pty Limited paid AU$25,200 infringement notice following an ACMA investigation that found that it had breached telemarketing laws.

» September—Lead My Way Pty Ltd paid AU$285,600 infringement notice following an ACMA investigation that found it had breached the DNCR Act by calling numbers on the DNCR.

» July—Service Seeking Pty Ltd paid AU$50,400 infringement notice following an ACMA investigation that found it had breached the Spam Act by sending SMS messages without consent, for failing to identify who authorised them and for not including an unsubscribe statement.

United Kingdom[33]

In 2017, 33,189 complaints were recorded by customers who received silent and abandoned calls. This showed a substantial decrease from 28% in 2015 to 22% in 2016, and an ICO reported a decline in unwanted marketing calls by 17% from 2016. Over time, Ofcom has refreshed its approach to enhance the environment from its current form.

ICO in action through Privacy and Electronic Communication Regulations 2018 (PECR)

According to the ICO report, by October 2018, 103 cases were under investigation for nuisance calls and spam emails, and formal enforcement action was taken against the organisations. Some particular cases were highlighted during the investigation, and a total of GBP310,000 in monetary penalties were issued :

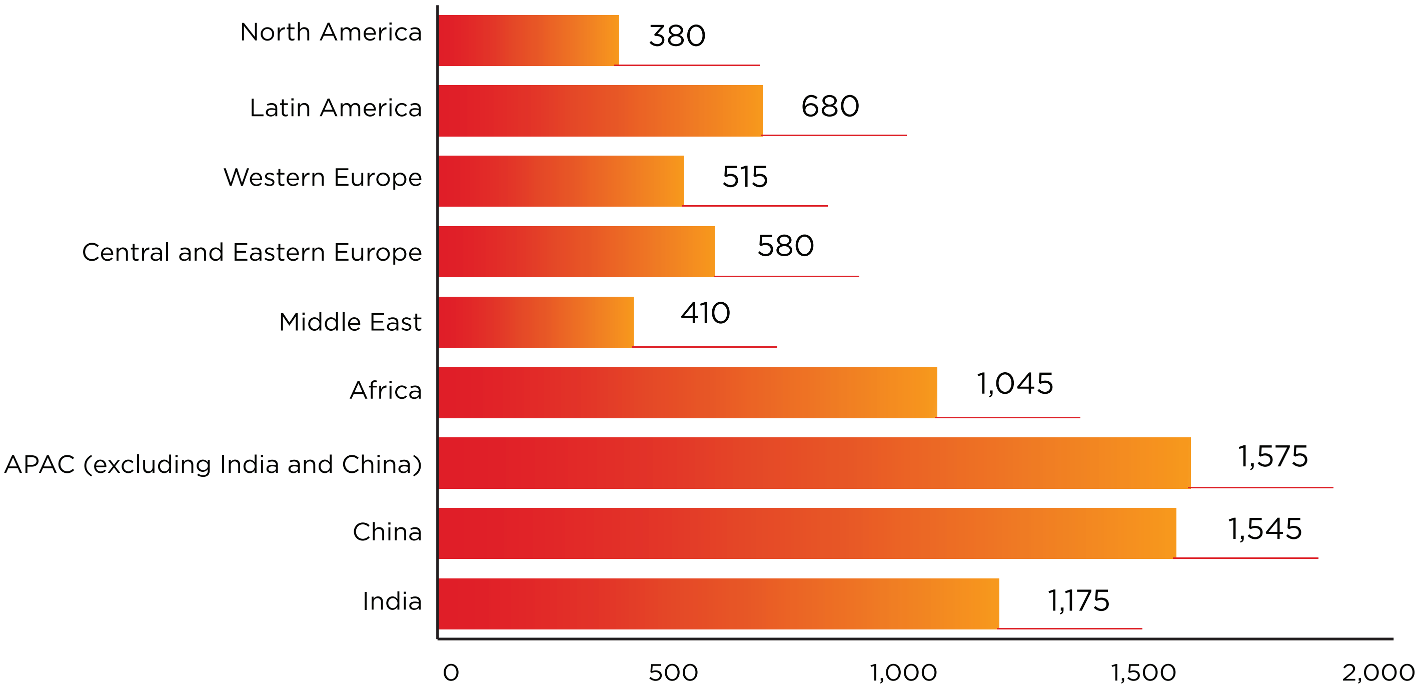
» Secure Home Systems and ACT Response Limited were levied a monetary penalty of GB80,000 and GBP140,000 respectively, for making calls to subscribers enlisted on the Telephone Preference Service.
» Boost Finance Limited was levied a monetary penalty of £90,000 for sending unsolicited email marketing.

Though there are opt-in systems in place for customers to submit their consents, these are predominantly recorded through verbal or written communications. These are difficult to trace, authenticate and maintain as verbal communications do not have a trail and hard copy paper trails are too cumbersome to manage and are prone to being misplaced or misused. Further, in case of a customer complaint, the details of the consent would not be traceable thereby leading to non-resolution of customers complaints. Inefficiencies in customer consent management and complaint redressal frameworks hamper user confidence and trust in the ecosystem.

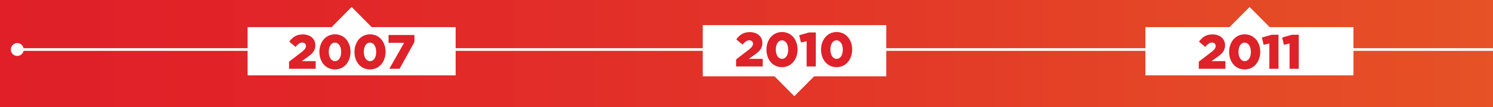
3.2 THE INDIAN CONTEXT

India is one of the most rapidly developing economies of the world. A 1.3 billion people strong country growing at a GDP of 8.2 per cent, India is one such market that business value the most in terms of potential businesses, expansion and even sustained businesses. India is also host to over a billion mobile phone subscriptions (1.1 billion) of which over 500 million are internet subscribers. With a tele-density of approximately 90—telecommunications services have definitely been the most pervasive and economical mode for businesses to reach out to their customers and markets.[35] India's smartphone shipments grew to almost 1.6 billion in 2017 devices shipped, while feature phone shipments rose 5% to 450 million devices.[36] The increasing penetration of mobile phones has successfully led to the widening scope for commercial communication through SMS and voice. Worldwide mobile internet users grew by 9.2% in 2017, while India

Mobile Subscription Q3 2018 (million)



3.2.1 Indian Regulations for Commercial Communication



The Telecom Unsolicited Commercial Communications Regulations (TUCCR)

- Every access provider to maintain a **National-Do-Not-Call registry (NDNC)** - private list of the subscribers not to receive commercial communications.
- Financial disincentives for non-compliance
- Framework for complaint redressal

Nearly **6 million** mobile subscribers enrolled themselves with the **National-Do-Not-Call registry** within just **10 days** of its launch. More than **15,418 telemarketers** registered within 3 months.

2011 Amendments

- Timings for communications to customers restricted to 0900 to 2100 Hrs.
- Time to update consumer preferences reduced from 3 months to 7 days
- Provision of the '140' series for ease in telemarketer identification
- Registration of SMS header format for commercial communications

The Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2010)

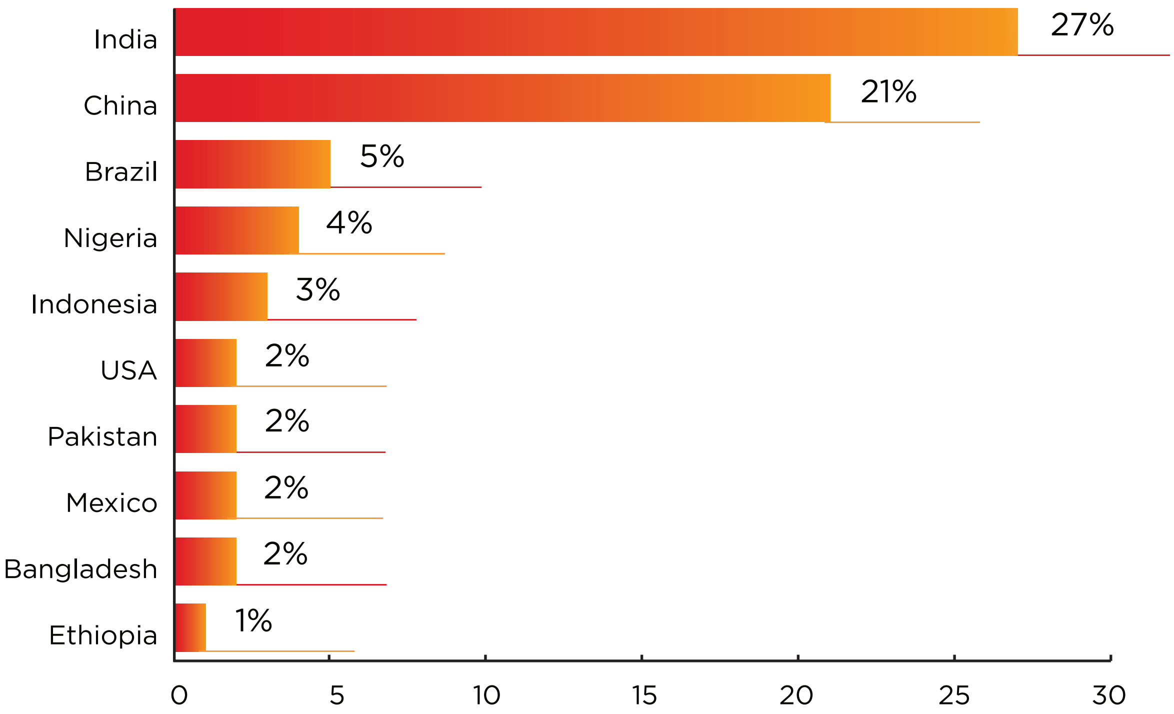
- Registration of consumer preferences on the National Customer Preference Register (NCPR)
- Deduction from the security deposit of registered telemarketers in case of non-adherence to the NCPR

grew at over double the rate at 22% , user base for commercial communication is only going to grow further in the coming years as well.[37] However, the huge volume of business communications have also driven the volumes of unsolicited commercial communication (UCC.) Spam, Phishing, Data brokerage and other fraudulent activities have become prominent forms of UCC in the ecosystem that remain unmitigated. This stressed the importance of a robust regulatory environment in order to place strict controls on entities and safeguard the interests of the customers.

In order to curb the inconvenience and distress caused to customers the Telecom Regulatory Authority of India notified the Telecom Unsolicited Commercial Communications Regulations (TUCCR) on 5th June 2007. Time and again TRAI has updated its regulations with regard to commercial communications and customer preferences primarily to empower customer choice while also maintaining the commercial interests of the players.

% age of new subscribers (2016-2020)

[37]



2012 Amendments

- Signature solution introduction to detect Unregistered Telemarketers (UTM).
- Higher BULK SMS tariffs
- Limiting multiple SMS's with a similar signature to 200 SMSs/ hour except for Registered Telemarketers (RTM)

2014 Amendments

- Transactional messages to incorporate details of sender entities, conditions for sending such messages and receiving such messages
- Introduction of options to receive replies of messages sent by RTMs

2012
2013
2014

2013 Amendments

- Allowed an individual to register a complaint on behalf of the another
- Disincentives to access providers allowing UTM activities

These regulations gave customers a choice to register their consents and preferences. As of 2016, however, customer consents and preferences were not updated in the NDNC, and NCPR registers on a real time basis further allowing telemarketers to continue sending commercial communications to customers. Further, consents were registered in an unverifiable and unauthenticated manner without any traceable and verifiable proof. Scrubbing techniques were also not the most efficient and in most cases failed to restrict sending messages to customers enlisted in the NDNC and NCRP registers.

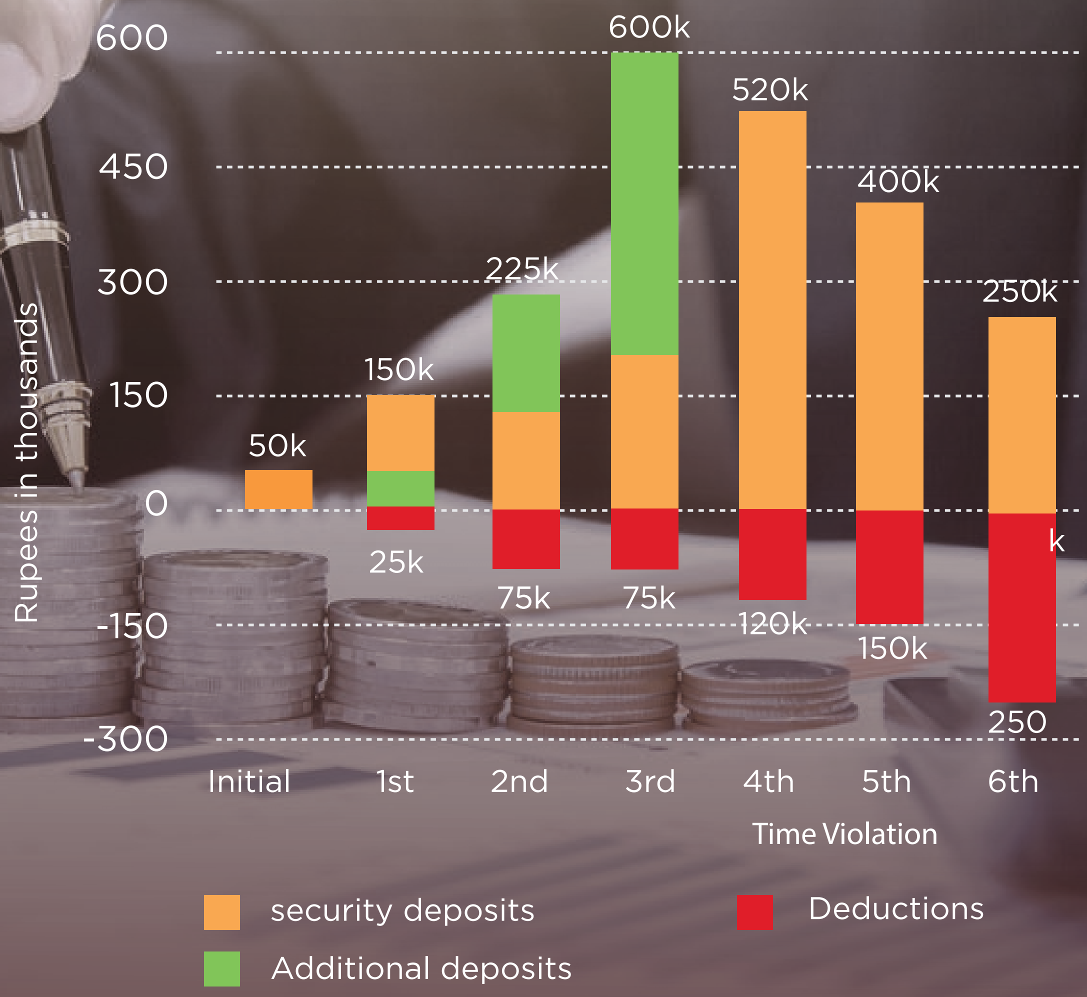
> **The delays in implementation of customer consent , lack of regulatory oversight and ineffective scrubbing controls, enabled unscrupulous telemarketers to exploit the system which severely impacted the user experience and trust in the control landscape. Id that a single opt-in process is not sufficient proof of prior consent.**

The financial disincentives and blacklisting of telemarketers introduced in the regulation were not effective in motivating players to comply with the requirements. The penalties imposed on the telemarketers were not even a fraction of the revenue the players were making. As of 2018, TRAI had blacklisted only 18 from a base of 8 thousand registered telemarketers. The many "second chances" and minimal penalty amounts allowed violating telemarketers to continue sending UCC. **Some success was met as approximately 1.4 million numbers were disconnected and about 460 thousand numbers were blacklisted up until 2017. Though these regulations and restrictions did reduce the nuisance created by UCC, they did not provide a well-rounded solution to the issues at hand.**[38]

Despite disconnecting more than a million telephone numbers, UCC Complaints were on a rise.

> **As per TRAI, approximately 2 million complaints were received up till July 2018 with another 40 thousand being added every month. The rise in customer complaints in addition to the lengthy resolution time of over 7 days led to negative customer experience.**

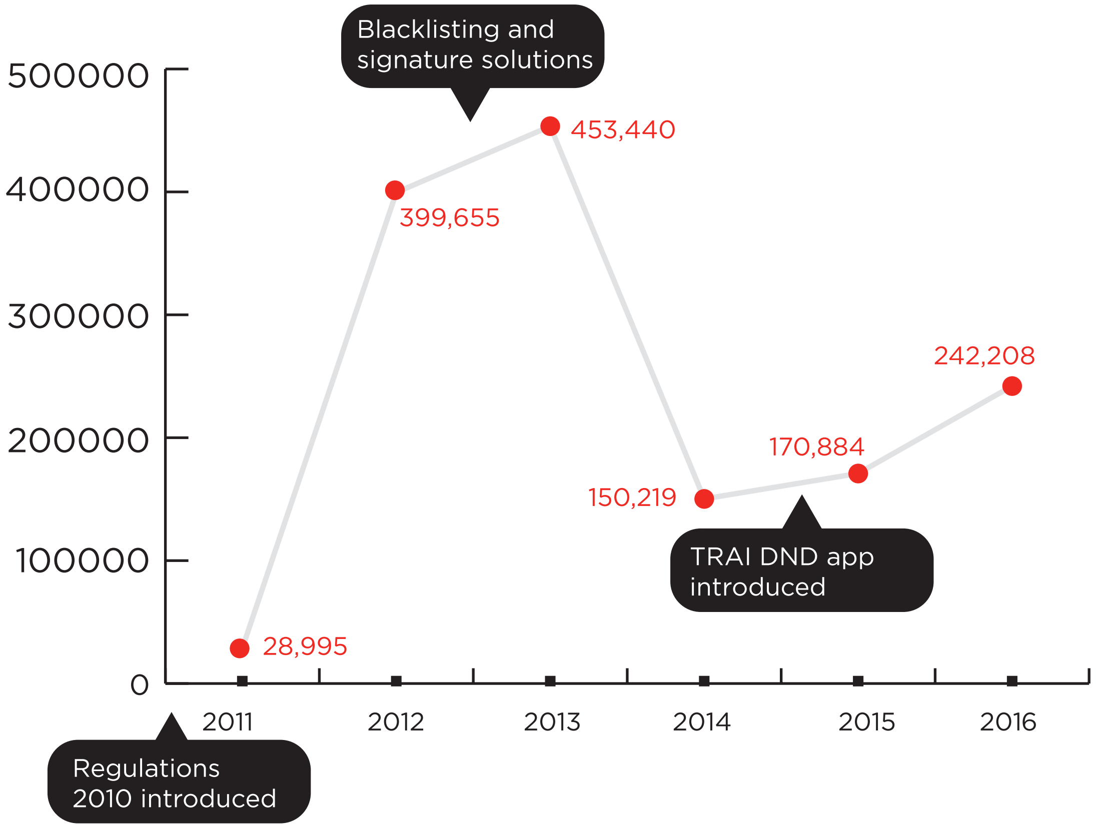
39 Security deposits and deductions



18 **Telemarketers blacklisted**

INR 3.71 **crores collected as Deductions**

After 6th violation, telecom resources of RTM are disconnected by all access providers and blacklisted for 2 years



UCC complaints over last few years

40

In 2017, market regulator Securities and Exchange Board of India (SEBI) felt the need to act on growing damage caused by fraudulent bulk messages. False market investment tips and information were actively shared through A2P SMS channels by unregistered and unknown senders to investors, thereby misleading the investors. SEBI sought TRAI's support in reducing the vulnerabilities of the securities market and control the financial loss caused to investors while ensuring investor confidence. The increasing need for a secure and robust regulation was becoming a necessity. With innovation and technological advancements in UCC in the form of silent calls, robocalls, botcalls, fake messages simulating authenticated transactions, etc. there was a requirement for technological advancement in the control landscape as well.

3.3 THE TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCE REGULATION 2018

The Telecom Regulatory Authority of India (TRAI), in its efforts to curb UCC framed and improved various amendments to the regulations regularly for over a decade. Despite all these efforts UCC related complaints were still on the rise and the issue still remained a pain-point at large.

Consequently, to address the issue with a more comprehensive and technology-driven approach, the TRAI initiated a consultation process on 14th September 2017 to seek inputs from stakeholders on how to overcome the problems and plug loopholes in the system.

On 19th July 2018, TRAI re-introduced TCCCPR as a more technology driven regulation than ever before.
The TCCCPR, 2018 inspired by RegTech, sets out to moderate and reduce UCC through the use of a permissioned and private Distributed Ledger Technology (DLT), or blockchain, to enforce regulatory compliance while allowing innovation in the market. Exhaustive registration process and recording of information on immutable blocks streamlines the availability of audit trail. The new regulation also provides for a wide range of customer preferences management processes which warrant near real time implementation as well. It also provides for the use of cloud-based solutions for handling complaints, registration of headers and preferences, and use of smart contracts for automatic allocation of roles between entities in the commercial communication ecosystem. Through AI and ML integration and signature solutions, the technology-based solutions are required to be tested in regulatory sandboxes under the oversight of the TRAI

01

Registration of Entities and Headers

Registration with access providers on DLT was mandatory for senders to be allowed to send out commercial communication. Such whitelisting activities require pre-checks for on-boarding entities thereby ensuring a verified and trusted source of communication. Through registration of headers on the platform, customers are able to clearly identify the entity and the type of business and message (promotional, service or transaction) being delivered. This enables customers to easily identify the purpose of the message thereby allowing them to

02

Registration of Content templates

To ensure flow of genuine information aligned to message labels, enterprises and telemarketers were mandated to register their content templates for SMS and voice as well. This ensured storage of information in an immutable manner while verifying the purpose of the template. This was also required for consent templates in order to ensure correct placement of suffixes. These were to provide customers the option to revoke their consent.

03

Registration of Customers Choices

The advantage of having a technologically enabled solution was the control that it brought to safeguard customers' consents and preferences. These were recorded on the DLT within 15 minutes upon being requested by the customer and enforceable within 24 hours. Customer were given the choice to set preference for industry category, mode of communication, time band and day and modify their preferences. Information with respect to registration, modification and revocation can be easily stored on the DL for any period of time as set by the operators. This provides users with clear, categorized and traceable information.

"Being in the banking Industry, we send sensitive information such as OTP, transaction and balance information to customers over SMS. Hence it is imperative that all customer communication channels must be secured and reliable over the globe.

I am happy to learn that with TRAI's new regulation, messages will be end-to-end encrypted and the brand/ Sender ID will not be compromised, empowering our customers to trust all branded communications and take further action on them without hesitation."

Dilip Pandya
Head - IT Support, Shared Services - Information Technology

Such platforms helped reduce the burden of complaints on the access provider. Whitelisting telemarketers, enterprises, content templates and mapping against preferences and consents along with scrubbing, allowed for the creation of preventive measures which would reduce UCC traffic significantly while enhancing customer security.

TCCCPR 2018, in the creation of a broad regulatory framework based on ecosystem consensus, allows access providers to play a co-regulatory role to implement through Code of Practices (CoPs).

As a result, requirements to be fulfilled by the senders would depend upon the CoPs of the specific access provider providing services to the sender. Additionally, in order to put a check on the nuisance caused by auto-dialers, silent or abandoned calls, TCCCPR 2018 prohibits senders from initiating calls with auto-dialers. Senders can use auto-dialers only after notifying the access provider in advance about the usage and about steps taken to maintain abandoned calls within limits provided for in these regulations or the CoPs.

> **Under TCCCPR 2018, customers may give their preference for receiving commercial communication through robo calls. The CoPs must account for reporting of unregistered entities found to be engaged in making such calls when brought to the notice of the access provider.**

In this manner, TCCCPR 2018 allowed for creation of a holistic regulatory environment among key stakeholders of the CC ecosystem – Access Providers, Telemarketers/ Aggregators, Enterprises and Consumers through a technology driven solution to enforce its provisions.

4

THE INDIAN CASE STUDY

TANLA'S PIONEERING SOLUTION TO CURB UCC

4.1 THE REGULATORY INITIATIVE

India by virtue of being the world's second largest telecom market by subscribers is an enormous opportunity for enterprises. The massive consumer base in India promises high prospects and sustainable growth. Having said that, the more than 1 billion telecom subscriber base in India warrants businesses to undertake extensive measures to ensure awareness of their business, products and/or services. This is where modern commercial communication methods play a vital role. The widespread use of commercial communication is accentuated by the fact that over 20 billion messages are sent in India alone in a month. A lot of these messages are not aligned with customer consents and preferences and are hence classified as UCC. Despite the prevalence of a "Do Not Disturb directory" or DND as it is referred to, unscrupulous elements have found ways to bypass the directory and target customers through UCC. There have been multiple instances of customer complaints describing irrelevant calls made to customer thereby breaching customer space and privacy.

Globally regulators, access providers and enterprises have been making efforts to control UCC; they have met with limited success as a comprehensive technology solution aligned with the regulatory aspects was not available so far.

The introduction of the TCCCPR 2018 requires implementation of the distributed ledger technology (DLT)/ blockchain and is aimed at creating a platform of trust, data privacy and security for all the stakeholders in the commercial communications ecosystem.

The spirit of the regulation was to curb UCC through the use of advanced technologies available such as blockchain to build trust and transparency in the ecosystem and use Artificial intelligence and Machine learning to significantly enhance the pattern matching and detection abilities for unsolicited communication

The key objectives being:

» Build trust across the ecosystem to safeguard the users and provide them with an appropriate degree of protection while enriching the customer experience
» Enable access providers to have access to the entities delivering commercial communication to avoid chances of financial disincentives on non-compliance to the regulation
» Promote easy entry of telemarketers and enterprises to allow more players to participate in the commercial communication ecosystem while adhering to the regulation

4.2 TANLA'S PIONEERING SOLUTION

Taking this as an imperative, Tanla has developed a cutting-edge technology solution, Trubloq, to counter all UCC challenges and to meet the discerning needs of the diverse clientele ranging from enterprises to carriers across geographies. **Serving approximately 840 million existing customers, predicted to migrate about 240 million preferences and over 15 billion consents, Trubloq is set to become one of the largest UCC stack providers globally.**

As a market leader, Tanla has been dedicated towards building a platform that caters to the needs of all players in the ecosystem. Determined to create an inclusive co-regulatory DLT environment, Tanla took upon the responsibility to make the implementation of the regulation a success. Tanla being a key player in the ecosystem understood not only the regulation very well but also how it could be made successful by involving all other players in the ecosystem. The key aspect was to build consensus among all the key stakeholders and ensure that implementation of the regulation would benefit all the ecosystem players and at the same time reduce unscrupulous elements. Tanla embarked on extensive consultations with the Industry and involved leading telecom players and enterprises in discussions to allay their apprehensions and provide clarity. It also commissioned an extensive market research through Nielsen to better understand the customer expectations and their problem areas. In addition to this, the company also looked up to the telecom regulator for further guidance about the compliance and technical aspects of the regulation.

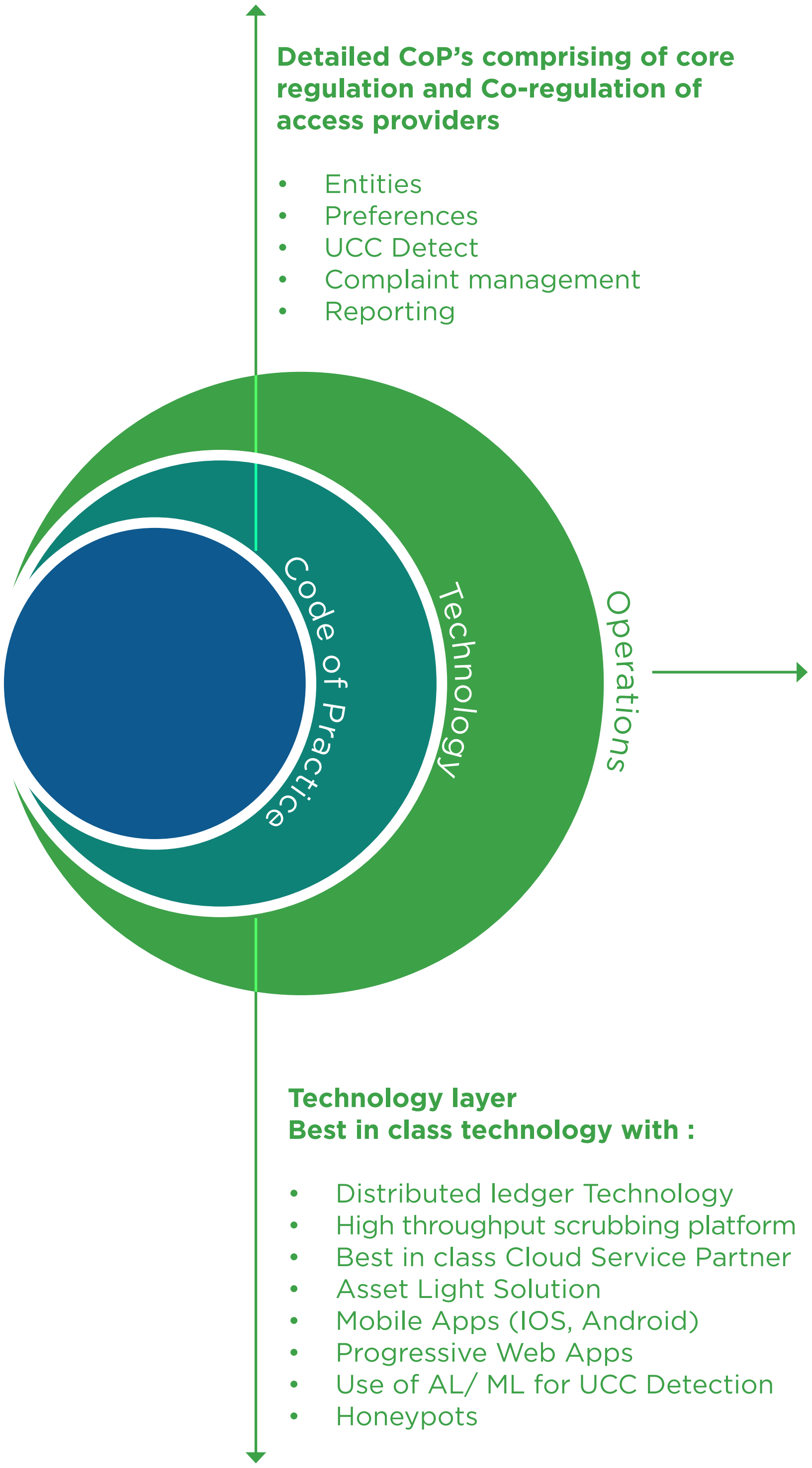
Post this Tanla embarked on a 7-month journey to be the first to market with a comprehensive solution that would cater to the regulatory requirements. This started by first building a comprehensive code of practice as mandated by the regulator on which the technology and the operations layers were further developed. This framework (refer diagram) depicts how all the aspects have been integrated for a sustainable solution.

> **Rather than spending time in reinventing the wheel, Tanla progressed fast by building the technical solution with expertise that was sourced from industry leading players including business consultants, blockchain developers and cloud service providers.**

This allowed Tanla to focus on its core competence i.e. omnichannel commercial communication and making sure that the solution was fully compliant with what the Indian regulator had envisaged.

Solution Framework

Operations Layer : Driven by comprehensive standard operating procedures



Detailed CoP's comprising of core regulation and Co-regulation of access providers

- Entities
- Preferences
- UCC Detect
- Complaint management
- Reporting

Technology layer
Best in class technology with :

- Distributed ledger Technology
- High throughput scrubbing platform
- Best in class Cloud Service Partner
- Asset Light Solution
- Mobile Apps (IOS, Android)
- Progressive Web Apps
- Use of AL/ ML for UCC Detection
- Honeypots

On-boarding entities

- Leverage our sales network
- Our strong aggregator relationships
- Establish a strong reseller network

Business Operations

- Registrars organization with comprehensive SOP's developed by our knowledge partners
- Dedicated team to detect UTM's and recommend action

Regulatory Assurance

- Dedicated team to resolve customer complaints
- Customized reports to operator and regulators
- Define KPI's like Complaints per million, TAT etc.

Technical Operations

- Automated tools for ticket creation to resolve Applications issues
- Networks & infra management
- Throughput management

Revenue Assurance

- Dedicated RA team with defined financial controls
- Leveraging smart contracts to automate controls
- Streamlined collections and payables

Technology

- Develop new use cases of block \chain
- Implementing changes/ upgrades to existing platform
- Ensuring compatibility with new technologies

The solution finally took shape and was named TRUBLOQ (Empowering Choices) and is the first of its kind in the global commercial communications ecosystem. Crafted with superior blockchain technology and integration capabilities with AI/ ML, Trubloq enables value creation for all while ensuring a trusted and reliable platform. This Solution is also supported by an app that customers can download on their devices and take back complete control of their preferences and consents as well as complaint management. For a smooth transition of the current ecosystem to the DLT platform, detailed migration planning was undertaken to transfer the existing data to the platform. These included migration of customer consents, preference and complaints and details of registered entities with TRAI registers.

By creation of a sandbox for testing of operational & compliance checks and controls, Trubloq led to the conception of a secure environment for the stakeholder consortium to participate in the usage of DLT networks.

Some of Trubloq's salient features are as follows –

01

Compliance Assurance: 100% stress free compliance to the regulation through creation of comprehensive governance framework in consensus with the ecosystem players.

02

Rich user interface: Developing user friendly interface with capabilities for customers to record their consents, preferences, complaints; telemarketers and enterprises to register themselves and their headers and content templates

03

Rapid Complaint Redressal: Customers can also easily file their complaints and grievances and in turn receive timely resolution.

04

Use of Artificial Intelligence (AI) and Machine Learning (ML): Use of AI/ML technology driven solutions to help:

» Identify trends with respect to attempts to send UCCs and report exceptions

» Identify and analyse the quantum of similar complaints with respect to UCC

05

Availability of Audit trail: Robust registration process and immutable recording on the blocks creates an audit trail for future references which subsequently assists in accurate fixation of accountabilities

06

Scrubbing rulesets: Trubloq aims to enhance its customers experience by disallowing exploitation of data privacy and data security. It ensures honouring of customers consents & preferences, while ensuring message delivery occurs for registered entities on the basis of registered headers in registered content templates.

07

Security features: Mobile number binding registration, OTP based authentication, exclusion list of headers, end to end encryption of messages are some of the key security and safety features which prevent malicious practices across the ecosystem.

SOLVING THE COMMUNICATION CRISIS

Trubloq is a blockchain- based stack that empowers individuals to truly own, control and manage their commercial communications, enabling businesses to build trusted relationships with their consumers.

Built for trust across ecosystem to safeguard users from fraudulent communication and enhance customer experience

Eliminate Phishing and other fraudulent activities through comprehensive mechanisms and content verification

Eliminate unregistered telemarketers using Honey pots, Cognitive computing and AI & ML

Zero tolerance to data privacy and security by ensuring customer data like consent and preference

End to end encryption of message content from sender to end user

Built for interoperability and engineered for universal compatibility with both legacy and ledger-based blockchain protocols

4.3 WHAT'S IN IT FOR ALL THE STAKEHOLDERS:

Trubloq at its core is a user friendly and a universally applicable solution that promotes a collaborative ecosystem and envisions to help channelize the objectives of the regulation towards creating a holistic and cooperative environment among all its stakeholders The solution's interoperability and transparent compliance to the regulation enable the creation of a consistent omni-channel experience benefiting all its stakeholders -

01 Customer

- Enables customers to clearly understand the purpose of consent requested and register the same on a Distributed Ledger (DL)
- Enables customers to choose from various categories for registration/ modification of preferences as well as their preferred channels and time bands to receive such communication.
- Ease in complaint registration through preferred channel of communication and faster complaint resolution system to address UCC complaints
- Digitally authenticated transactions to ensure consent, preference and complaints have been registered by the actual user

02 Access Providers

- Reduce levy of financial disincentives caused by UTMs sending UCC
- Easily trace defaulting telemarketers or enterprises through UCC detect and take necessary remedial action
- Setting up a systematic customer consent, preference and complaint registration facility
- Reduction in operators expenditure on data security solutions and architecture by providing a one stop shop and in turn reducing UCC and maintaining data privacy
- Real time reporting, red flagging and dash boarding of the complaints and defaulters
- Customer satisfaction due to enhanced user experience thereby creating goodwill for the access provider

03 Telemarketers

- Easy onboarding process and minimal upfront cost thereby enabling telemarketers to enter the market faster
- Strengthening regulatory compliance by conducting pre-requisite checks before registering telemarketers
- Enabling efficient message delivery planning as per registered customer preferences
- Cognitive Computing and Machine learning capabilities to perform datamining to provide customized reports/ Trends

04 Enterprises

- Better conversion rate due to clear and targeted customer communication
- Improved sales as a result of communication with targeted customer base at time preferred by them, through their choice of channel of communication
- Safe and secure maintenance of customer data
- Easy registration of headers, content and consent templates

From the share of volume, the best in class technology, enhanced scrubbing mechanisms and adequate spam detection measures it can very well be inferred that implementation of Trubloq in the ecosystem would be one of the most prudent ways of curbing UCC and its impact for all players. Set to be the largest such use case of technology in a regulatory aspect, Trubloq promises to be the missing piece from the ecosystem puzzle.

THE WAY FORWARD

The potential of constant reinvention of modes to communicate with end customers coupled with the increase in user convenience as well as ensuring brand loyalty has created a strong base for commercial communication. Innovational evolution in channels such as SMS, voice and emails are key enablers for continuous and seamless interaction between enterprises and their end customers. The advent of channels such as RCS are set to lead the way forward for rich customer engagement.

> **The sustained eminence of such channels of communication are recognized through their 5-10 per cent predicted traffic CAGR from 2007 till 2022. Set to cross the USD 26 billion mark in revenue by 2022, such channels continue to enable key players in the ecosystem to develop successful monetization strategies.**

However, where there are high revenues, frauds stealthily follow. The problem of unsolicited commercial communication associated with frauds by unscrupulous organisations, increasing spam and fake news cases, etc. is an ever-growing risk. This has made it imperative to safeguard the players in the ecosystem and most importantly, the customers from becoming easy preys to unsolicited commercial communication. Adoption of security measures and mitigating controls by the key players, have allowed them to confront this growing problem. However, these measures are required to be adopted collaboratively by all the players in order to enhance customer protection. Additionally, regulators today, globally, are collectively focusing on empowering choices of end customers. The need of the hour for all enterprises, is to make choices in terms of consent and preferences available to customers while ensuring compliance to the regulation, as the commercial communication ecosystem rapidly progresses.
Regulators across the world are driven to ensure protection of customers' interests, experience and data exposure. While regulators are proactively making efforts to address customer's difficulties they are also focusing on creating a balance within the ecosystem. However, it is required for regulators to go further than simple application of the law. To attain an adequately functioning ecosystem, regulators need to enthusiastically update their regulations while taking into account the use of technology for unethical activities by individuals and organisations. Complementary regulatory mechanisms such as co-regulation and self-regulation are gradually being imbibed by regulatory authorities across the world. Such initiatives would be beneficial in delegating regulatory responsibility to all stakeholders while ensuring customized and flexible adoption of the same.

With customers at the core of key regulatory amendments and initiatives, regulators have allowed for pro-active collaboration among key players in the ecosystem to take equal responsibility to sanitise and establish proper codes of conduct, thereby protecting the essence and dignity of commercial communication. Regulatory bodies like India's TRAI through mandates such as TCCCPR 2018, have allowed for the existence of control landscapes to be technologically equipped in order to strengthen their protective measures for customers and players of the ecosystem alike. Such exemplary regulatory initiatives have set a case for global adoption. This in turn, will help operators save millions by tackling the threat of fraud, spoofing and data privacy which happens at the expense of their network in a much more compliant environment. This will also help in controlling the illegal entry points for unregistered telemarketers and curb the penetration of unwanted messages leading to uniform distribution of tailored content aligned with customer preferences with proper consent. The onset of technological convergence requires a forward-looking policy to ensure adoption of healthy business practices, mitigation of data leakage, fraud monitoring, and above all, honouring customer preferences. The introduction of such technologically enabled solutions for regulatory compliance use cases, popularly known as RegTech, has led to the evolution of the regulatory landscape. Adoption of this in tandem with stringent regulatory guidelines is considered as a significant milestone in addressing the challenges arising from UCC. Innovative technologies like DLT, and cognitive computing would enable facilitation of a multi-layered solution, positively impacting the current state of digital communication and securing the trust of billions of subscribers around the world.

The implementation of such blockchain-enabled solutions while setting an example for a successful alliance of regulation with technology, also allows a holistic approach by focusing on enhancement of the commercial communication value chain while protecting and securing the interests of billions. Secure and safe storage of customer's preferences and digital consent on such platforms allows for real time activation, building trust and enabling businesses to gain data and control information in a secured way. Embracing such technology is the way forward in empowering choices while driving monetization in the commercial communication space. Solutions such as Trubloq, born from forward looking regulations are aligned to this vision, while driving monetization in the commercial communication space. Such platforms are unique examples of robust and scalable technologies set out to make the vision of the regulators a reality.

Technologically enabled frameworks are the future of effective technology enabled regulation. Set to help in re-establishing the trust of customers by protecting their data, recognising and respecting their consents and preferences, this will empower them as active participants in the ecosystem.

Adoption of such technology will only contribute and fuel the growth of commercial communication without hampering user experience. Such technologically advanced use cases can enhance the degree of trust within the ecosystem, and pave the way forward for enterprises in revamping their digital strategies. This in turn will help boost their revenues and allow enterprises to gain better insights while obtaining a granular understanding of customer choices without invading customer space and privacy. For all players to be end winners, it is important for the regulation and its solutions to evolve and thrive as per the changes in customer behavior and technology. Together, this will set the pace for enablement of an all-inclusive and well-rounded framework while ensuring that the customer feels empowered, respected and secured, without discounting the commercial interests of other players..

Thus, for sustained growth of commercial communication, empowering customer choices is quintessential as a way forward.

GLOSSARY

S.No.	Abbreviation	Full Term
1	5G	Fifth Generation
2	A2P	Application-to-person
3	ACMA	Australian Communications and Media Authority (Australia)
4	AI	Artificial Intelligence
5	APAC	Asia-Pacific
6	API	Application Programming Interface
7	BEC	Business Email Compromise
8	BFSI	Banking, Financial Services and Insurance
9	CAGR	Compound annual growth rate
10	CAN-SPAM	Controlling the Assault of Non-Solicited Pornography And Marketing (United States)
11	CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
12	CASL	Canadian Anti-Spam Law
13	CC	Commercial Communication
14	CEO	Chief Executive Officer
15	CoP	Code of Practice
16	CRM	Customer Relationship Management
17	CRTC	The Canadian Radio-television and Telecommunications Commission
18	DAAP	Digital Audio Access Protocol
19	DDoS	Distributed Denial of Service
20	DL/DLT	Distributed Ledger/ Distributed Ledger Technology
21	DNCR	Do Not Call Registry
22	DND	Do Not Disturb
23	DoT	Department of Telecommunications, India
24	EU	European Union
25	FTC	Federal Trade Commission (United States of America)
26	Gbps	Gigabits per second
27	GDPR	General Data Protection Regulation
28	GMAIL	Google Mail
29	GSM	Global System for Mobile
30	HSBC	Hongkong and Shanghai Banking Corporation
31	ICO	Information Commissioner's Office (United Kingdom)
32	ID	Identity Document
33	INR	Indian Rupee
34	IoT	Internet of Things
35	IP	Internet Protocol
36	IRS	Internal Revenue Services
37	ISPA	The Internet Service Providers' Association of SA (South Africa)

38	IUC	Interconnection Usage Charges
39	IVRS	Interactive Voice Response Systems
40	KPI	Key Process Indicator
41	M2M	Machine-to-Machine
42	MII	Ministry of Information Industry (China)
43	ML	Machine Learning
44	MNO	Mobile Network Operator
45	NCPR	National Customer Preference Register
46	NDNC	National-Do-Not-Call registry
47	NHS	National Health Service (United Kingdom)
48	Ofcom	Office of Communication
49	OTT	Over the top
50	P2P	Person to person
51	PECR	Privacy and Electronic Communications Regulations (United Kingdom)
52	Q2	Second Quarter
53	RBI	Reserve Bank of India
54	RCS	Rich Communication Services
55	RegTech	Regulatory Technology
56	RTM	Registered Telemarketers
57	SEBI	Securities and Exchange Board of India
58	SIM	Subscriber Identification Module
59	SMS	Short Message Service
60	SOP	Standard Operating Procedure
61	SS7	Signaling System 7
62	TAT	Turn Around Time
63	TCCCPR	The Telecom Commercial Communication Customer Preference Regulations
64	TM	Telemarketers
65	TMSE	Transactional Message Sending Entity
66	TPS	Transactions per second
67	TRAI	Telecom Regulatory Authority of India
68	TUCCR	The Telecom Unsolicited Commercial Communications Regulations
69	UCC	Unsolicited Commercial Communication
70	URL	Uniform Resource Locator
71	USCIS	US Citizenship and Immigration Services
72	USD	United States Dollar
73	UTM	Unregistered Telemarketers
74	VNO	Virtual Network Operator
75	VoIP	Voice over Internet Protocol

REFERENCES

1 The Telecom Commercial Communication Customer Preference Regulation 2018 | May 29, 2018

2 Digital Marketing vs Traditional Marketing: Which Produces Better ROI - LYFE MARKETING | July 20, 2018

3 2018 Digital Yearbook - We are social and Hootsuit | Jan 30, 2018

4 GSMA Intelligence | Jun 15, 2017

5 New Ovum Report Reveals Strong Enterprise Appetite for RCS Messaging and Chat Bots While Confirming the Continued Growth of A2P SMS - CISION | Jul 20, 2017

6 Tap Into The Marketing Power of SMS - Gartner | Nov 3, 2016

7 RCS MESSAGING REVENUES TO REACH $9 BILLION BY 2022, AS OPERATORS CAPITALISE ON NEW ENGAGEMENT CHANNELS - Juniper Research | May 22, 2018

8 Email Statistics Report, 2018-2022 - The Radicati Group,Inc

9 Digital in 2017: Global Overview - We are social and Hootsuit | Jan 24, 2017

10 Global A2P SMS messaging forecasts by country, 2017-2022 Databook - Mobilesquared

11 The Future of Business Messaging - Mobilesquared, GSMA | Nov 15, 2018

12 MEF - A2P Monetization Report November 2018

13 Truecaller Insights report, 2018

14 Global spam categories 2017 - Statisa

15 Nationwide Robocalls Data, 2018 - Robocalls index

16 50+ phishing statistics and facts for 2017-2018: The rise of SSL-secured phishing - Comparitech | Aug 28, 2018

17 Grey routes: how to detect and monetize - GMS worldwide | Sep 25, 2018

18 Sim box fraud unearthed in Hyderabad - Times of India | Apr 13, 2018

19 Premium SMS Malware 'ExpensiveWall' Infects Millions of Android Devices - Threat Post | Sep 14, 2017

20 NHS data breach affects 150,000 patients in England - BBC News | Jul 2, 2018

21 Scam Alert: Fake Banking Apps Tricking Consumers - Experian | Mar 9, 2018

22 1 out of 4 customers is a victim of online fraud: Experian report - The Economics times | Jun 25, 2018

23 Times of India

24 15 people, five Indian BPOs, indicted in massive call center - times of India | Sep 8, 2018

25 24 Arrested For Duping Microsoft Customers From Fake Call Centers: Police - NDTV | Oct 06, 2018

26 Don’t return that missed call! - Times of India | Feb 22, 2015

27 ISPA

28 Mondaq - Canada: Canada’s Anti-Spam Legislation: What You Need To Know To Comply With CASL

29 FTC - Can spam act

30 OFCOM, ICO

31 “sampi.co - China Email Marketing and Chinese Anti-Spam Laws
Lightspandigital - What You Need to Know About Anti-Spam Laws Around the World”

32 AMCA - Protect yourself from spam

33 GDPR org - GDPR Key Changes

34 OFCOM - Nuisance calls joint action plan 2018

35 Hindustan times - India’s mobile subscriber base to touch 1.42 billion by 2024; 80% to use 4G

36 TRAI- performance indicator report June 2018.

37 Forbes - Explaining The Booming Market For ‘Dumb Phones’ In India

38 MMAGLOBAL - MMA mobile ecosystem report 2018

39 TRAI - UCC - Consultation paper

40 TRAI - TCCCPR 2018

tanla

Tanla started its journey as the new millennium set in with a small group of mobile messaging experts, with base in Hyderabad, India, to create a world-class messaging service. Today, Tanla is a global leader in its domain as one of the largest Cloud Communication providers, handling over 100 billion business communications annually. Tanla is innovating the way the world communicates, continuously raising the bar through enhanced speed, ease and simplicity of Cloud Communication solutions, adopting cutting-edge technologies to meet the discerning needs of a diverse clientele, from enterprises to carriers across geographies. Tanla is a public limited company listed on leading Indian stock exchanges (BSE CODE: 532790 and NSE: TANLA).

CORPORATE CONTACT

TANLA SOLUTIONS LIMITED
TANLA TECHNOLOGY CENTRE
MADHAPUR, HYDERABAD,
INDIA - 500081

CIN: L72200AP1995PLC021262

Follow us on

DISCLAIMER

The report is prepared by Tanla Solutions and intended for limited distribution.

The material in the report is obtained from various sources (owner). We have taken reasonable care to ensure that, and to the best of our knowledge, material information contained herein is in accordance with the facts and contains no omission likely to affect its understanding. The contents of this report are not to be construed as legal or business advice.

Tanla acknowledges and agrees that the content (e.g. reports graphs, images, logos etc.) and all rights therein, including, without limitation, copyrights) belongs to and shall be the sole and exclusive property of the owner.