IN THE HIGH COURT OF DELHI AT NEW DELHI
CIVIL EXTRAORDINARY JURISDICTION
WRIT PETITION (CIVIL) NO. ___ OF 2020

IN THE MATTER OF:

One97 Communications Limited &Anr. …Petitioners

VERSUS

Union of India &Ors. … Respondents

WRIT PETITION UNDER ARTICLE 226 OF THE CONSTITUTION OF INDIA SEEKING THE ISSUANCE OF AN APPROPRIATE WRIT, ORDER OR DIRECTION IN THE NATURE OF MANDAMUS, OR ANY OTHER APPROPRIATE WRIT ORDER OR DIRECTION TO, INTER ALIA

a) DECLARE THAT REGULATIONS 25(5) AND 25(6) OF THE TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCES REGULATIONS, 2018 INSOFAR AS THEY ALLOW INADEQUATE AND THE IMPOSITION OF A GRADED PENALTY ON IDENTIFIED UNREGISTERED TELEMARKETERS AS UNCONSTITUTIONAL AND ULTRA VIRES THE TELECOM REGULATORY AUTHORITY OF INDIA ACT, 1997;

b) DIRECT THE RESPONDENT NO. 2AUTHORITY TO ENSURECOMPLETE AND STRICT IMPLEMENTATION OF PROVISIONS OF THE TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCES REGULATIONS, 2018 AND ANY OTHER RELATED REGULATIONS ISSUED FROM TIME TO TIME TO CURB FRAUDULENT UNSOLICITED COMMERCIAL

COMMUNICATION SENT OVER THE RESPECTIVE NETWORKS OF THE RESPONDENT TELECOM SERVICE PROVIDERS;

c) DIRECT THE RESPONDENT NO.2AUTHORITY TO TAKE ACTION AGAINST THE RESPONDENTS NO. 3 TO 9 TELCOSUNDER REGULATIONS 21, 27 AND 28, FOR VIOLATIONS OF THEIR PRIMARY OBLIGATIONS OF PREVENTION AND VERIFICATION UNDER THE TELECOM COMMERCIAL COMMUNICATIONS CONSUMER PREFERENCES REGULATIONS, 2018;

d) DIRECT THE RESPONDENT NO.1 DEPARTMENT TO TAKE ACTION TO ENSURE THAT NO SIM CARD IS SOLD WITHOUT PROPER VERIFICATIONBY EFFECTIVE IMPLEMENTATION OF THEDEPARTMENT OF TELECOMMUNICATIONS CIRCULAR DATED 09.08.2012TITLED *"INSTRUCTIONS ON VERIFICATION OF NEW MOBILE SUBSCRIBERS (PRE-PAID AND POSTPAID)"*;

e) DIRECT THE RESPONDENT NO.1 DEPARTMENT TO ENSURE EFFECTIVE IMPLEMENTATION BY THE RESPONDENT TELCOS OF THEIR OBLIGATIONS UNDER THEIR UNIFIED ACCESS LICENSE AGREEMENTS PERTAINING TO VERIFICATION AND REPORTING OF FRAUDS TAKING PLACE OVER THEIR NETWORKS;

MOST RESPECTFULLY SHOWETH:

1. The Petitioner No. 1, One97 Communications Limited, is a company incorporated under the Companies Act, 1956. The Petitioner No.1 is the owner of the consumer brand 'Paytm' and is also India's largest mobile first financial services / commerce platform offering payments, banking, lending and insurance. Being the brand owner and the proprietor of the "Paytm" brand, the Petitioner No.1 has all the right, title and interest in the trade-marks, service-marks, names, symbols, design logos, artwork and other related intellectual property rights in the "Paytm" brand. The Petitioner No. 1 has its own customers and also licenses the Paytm brand to its associate companies, including Petitioner No. 2.

   The Petitioner No.2, Paytm Payments Bank Ltd., is a Banking Company which was granted a license in 2017 from the Reserve Bank of India to carry on a 'payments bank' business. The Petitioner No.2 serves around 300 million customers across India and It delivers banking products and services to its customers through the Paytm Mobile App.

2. The present Writ Petition under Article 226 of the Constitution of India has been filed by the Petitioners on account of the failure of the Respondent No. 3 to 9 Telecommunication Service Providers to comply with the provisions of, and the Respondent No. 2 Authority to fully implement the statutory and technological architecture provided under the *Telecom Commercial Communications Customer Preference Regulations, 2018*(hereinafter,"TCCCPR 2018"). This has resulted in a rise in fraud through Unsolicited Commercial

Communication ('UCC') and phishing activities against the Petitioners' customers and impacting the brand of Petitioner No. 1, by fraudsters duping the customers into believing that they are the representatives of the Petitioners.As has been reported by the Times of India's Ahmadabad Mirror on 23.05.2020, three different complaints totalling Rs. 12.4 lakhs have been registered over a span of three days in Ahmedabad alone, where the son of a former Supreme Court Judge, an orthopaedic surgeon, and a senior citizen, were defrauded using a fraudulent link that sought an update on their Patym Wallet KYC norms.

3. Petitioner No.1 seeks the intervention of this Hon'ble Court to protect its business reputation and the severe damage caused to the "Paytm" brand as such instances being material in number and severity, adversely affect the Petitioner No. 1 and the "Paytm" brand. Moreover, this causes customers to lose faith in both Petitioner No. 1, its group company licensees and Petitioner No. 2, impacting the "Paytm brand" in the process, the barometer of trust being very critical for entities operating in India's ever growing and extremely competitive financial services / digital payments space. The Petitioner No. 2 seeks the intervention of this Hon'ble Court to protect millions of its customers, too many of whom have been defrauded by the activity of phishing taking place using the telecommunications services as SMS and Calls.

4. Apart from seeking effective implementation of the TCCCPR, the Petitioners have also challenged the constitutionality of Regulations 25(5) and 25(6) insofar as they pertain to the

penalties to be imposed uponunregistered telemarketers. By way of the present Petition the Petitioners have also assailed the failure of the Respondent No.1 Department to curb the sale of sim cards without proper verificationas stipulated in the instructions on verification of new mobile subscribers issued by Respondent No.1.

5. The Respondent No.1 Department of Telecommunications is the Department that grants the Unified Access Licenses (UALs) to the Respondents Nos. 3 to 9Telcos(and monitors the Telcos' adherence to their UALs).The Respondent No. 2 Telecom Regulatory Authority of India (hereinafter "TRAI") is the governmental regulatory body of the Telecom Industry and was constituted under the Telecom Regulatory Authority of India Act, 1997 (hereinafter 'TRAI Act'). Itsstated purpose is protecting the interests of consumers and service providers of the telecom sector and to promote and ensure orderly growth of the sector. In exercise of its powers under the TRAI Act, 1997, the Respondent No. 2 authority issued the TCCCPR 2018 which casts an affirmative statutory obligation on the Respondent No. 2 authority, as well as the Respondent No. 3 to 9Telcos to address phishing complaints from consumers. The Respondent No. 3 to 9 Telecommunication Service Providers (hereinafter 'TSPs'/ 'Telcos') are service providers whose networks are being used to send unsolicited commercial communication to the subscribers/ customers of these TSPs/ Telcos, who in the present case are also customers of the Petitioners. The Respondent Telcos carry out a public function as held in a catena of judgments, which have

been more specifically dealt with in the grounds of the present Writ Petition. As such, the writ petition under Article 226 of the Constitution of India is maintainable against the Respondent No. 1 &2 authority, as well as the Respondent No. 3 to 9 Telcos.

6. It is submitted that due to the Respondents' failure to provide and regulate its services, and to fully implement the TCCCPR 2018 and other related Directions and Circulars issued by Respondents Nos. 1 and 2,customers of the Petitioners and their associate companies/ related parties/ group companies have been receiving spam, or fraudulent &unsolicited commercial communication in the form of messages and phone calls from entities using message headers/ sender IDs/ SMS content deceptively similar to the Petitioners and its associate companies/ related parties/ group companies. Senders of such fraudulent and unsolicited commercial communication are also in other ways misrepresenting themselves to be "Paytm"employees.

What is Phishing?

There are several ways in which senders of such fraudulent messages and phone calls are "phishing" the bank details ofcustomers of the Petitioners and their associate companies/ related parties / group companies. Phishing is a technological attack often used to deceive a user into divulging data, including confidential bank details, passwords, login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening a text message or to

supply confidential information over the phone. The recipient is then tricked into clicking a malicious link, or dialling a number or orally communicating confidential information which can lead to the installation of mirroring apps, malware or other modes to reveal sensitive information which then allows the fraudster to withdraw funds from the victims' bank account.An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds. The Petitioners and others succumbing to such an attack are secondary victims, typically sustaining financial losses in addition to declining market share, reputation, and consumer trust. As a result of this phishing activity, several customers of the Petitioners have till date cumulatively lost about Rs. 10crores (approx).

Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR 2018)

7. The TCCCPR 2018 was issued by the Respondent No. 2 Authority to ensure standards of quality of services to be provided to consumers by Telcos, by laying down a mechanism to protect consumers from unsolicited commercial communication ('UCC'). Commercial communication is defined as any communication (text or voice) using telecom services, to advertise or solicit business for any purpose. Commercial communication has also been distinguished from transactional messages and calls (i.e. non-promotional communications) and service messages/calls, which are specifically excluded from the definition of UCC (Reg. 2(bw)). The TCCCPR 2018 regimeregulatesthe sending of commercial communication to consumers, with an aim to balance the consumers' rights to

privacy and safetyandthe legitimate commercial interests of businesses, by adopting a two-pronged approach of prevention and penalisation, namely:-

i. Consumers have the right to register their preferences (or lack thereof) to receive commercial communications andevery Telco isobligatedto ensure that there is no delivery or blocking of commercial communication to its subscribersin contravention to their registered preferences; and

ii. Every Telco is obligated to ensure the identification and verification of all commercial communications carried out over its telecom network by mandating the registration (using Distributed Ledger Technologies) of all entities wishing to send commercial communications as Registered Telemarketers (RTMs), while prohibiting the sending of any commercial communication by an UTM (Reg.32)

8. The overarching purpose of the regulatory framework which has the force of statute, therefore, is to protect consumers from UCC, of which fraud is the most damaging result, while ensuring that legitimate business relationships (whether transactional or service related) and legitimate promotional activities (through registered sender(s) in accordance with consumer preferences) may continue unhindered. However, despite this relatively robust regime, the failure of the Respondents to adhere to and effectively implement the same is resulting in an alarming rise in phishing and related

cybercrimes through the mode of spam/ Unsolicited Commercial Communication, thus necessitating the intervention of this Hon'ble Court

Jurisdiction of this Hon'ble Court

9. It is submitted that this Hon'ble Court has the jurisdiction to entertain the present Petition under Article 226 of the Constitution of India since:

    i. the nature of the relief(s) sought by the Petitioners i.e. the declaration of unconstitutionality of a part of the TCCCPR, and directions to be issued to the Respondent No.2 to ensure implementation of the TCCCPR are not amenable to the jurisdiction of the Ld. Telecom Disputes Settlement Appellate Tribunal (TDSAT); and

    ii. The Petitioners in any event, are barred from raising a dispute before the Ld. TDSAT under Section 14 of the TRAI Act.

10. It is a settled position of law that Tribunals like the Ld. TDSAT are creatures of their parent statutes (here, the TRAI Act), and therefore, such Tribunals cannot exercise any jurisdiction that has not been specifically conferred on them by the parent Statute. In the context of the Ld. TDSAT and the TRAI Act, it has been held by the Hon'ble Supreme Courtin***Bharat Sanchar Nigam Limited v. Telecom Regulatory Authority of India*** 2014 (2)SCJ 301 that the Ld. TDSAT is not competent to decide the vires of any Regulations framed by TRAI under Section 36 of the TRAI Act.

Thus,thevires of the TCCCPR (which is under challenge in the present Petition), having been framed by the Respondent No.2 Authority under Section 36 of the TRAI Act, cannot be looked into by the Ld. TDSAT.

11. In addition, the present Petition seeks that directions be issued to the Respondent No.2 Authority to ensure compliance and implementation of the TCCCPR by the Respondent Nos. 3 – 9Telcos, by inter alia, taking action against the said Telcos under Regulations 27 and 28 of the TCCCPR, so as to curb the fraudulent and phishing activities taking place through unsolicited communications over the Telcos' networks.It is submitted that the Ld. TDSAT is not empowered under the TRAI Act to issue directions to the Respondent No.2 Authority in original jurisdiction under S. 14 (a) (as opposed to Appellate jurisdiction against orders/ decisions/ directions of TRAI under S. 14(b)). The Ld. TDSAT, in its decision in ***Tamil Nadu Progressive Consumers Centre v. Ministry of Information and Broadcasting*** (Petition No. 60/2010) had issued certain directions to the Respondent No.2 Authority to ensure the implementation of the Quality of Service Regulations issued by the Respondent No.2 Authority in 2007.The said decision was challenged by the Respondent No.2 Authority before the Hon'ble Supreme Court in ***Telecom Regulatory Authority of India v. Tamil Nadu Progressive Consumers Center***(Civil Appeal No. 9035/2011), which vide Order dated 14.11.2011 stayed the operation of the TDSAT's decision. Thus, it is submitted that as on date the Petitioners cannot approach the Ld. TDSAT to seek the relief(s) claimed.

12. Further, it is submitted that under Section 14(a) of the TRAI Act, the TDSAT is empowered to decide any dispute raised only by licensor, licensee, service provider, or a group of consumers. The Petitioners, being neither a licensor, licensee or service provider as defined in the TRAI Act, nor a group of consumers, is therefore barred from raising any dispute before the Ld. TDSAT.

13. Thus, it is submitted that it is only this Hon'ble Court that, in exercise of its writ jurisdiction under Art. 226 of the Constitution, is competent to grant the relief(s) claimed in the present Petition.

OVERVIEW OF FACTS

14. The facts which have led to the filing of the present writ petition are as follows:

a. In order to deal with the menace of unsolicited commercial communication, the Respondent No.2 Authority notified the Telecom Unsolicited Commercial Communications Regulations 2007 (hereafter, '2007 Regulations') which envisaged the establishment of a National Do Not Call Registry to facilitate consumer registration of preferences against UCC.

b. The 2007 Regulations were superseded by the issuance on 01.12.2010 of the Telecom Commercial Communication Customer Preference Regulation 2010 (hereafter, '2010 Regulations') which introduced, inter alia, the mandatory requirement of registration of telemarketers. The 2010

Regulations underwent a number of amendments over the years

c. Pursuant to the decision of the Hon'ble Supreme Court dated 27.04.2011 in ***AvishekGoenka v. Union of India*** **(**W.P. (C) No. 285/2010), the Respondent No.1 Department issued a circulartitled*"Instructions on Verification of New Mobile Subscribers (Pre-paid and Postpaid)"*(hereinafter, 'DoT SIM verification Circular, 2012) dated 09.08.2012. The said Circular laid down the protocol to be followed by the Telcos before the issuance and activation of a sim card and prohibited the sale of pre-activated Sim cards. The sale of such pre-activated Sim card attracted a penalty of Rs. 50,000 on the Telco per Sim card. Clause 6 of the said Circular also prohibited the issuance of bulk mobile connections (i.e. 10 or more) to individuals, and strictly regulated the verification process for bulk connections in the case of companies/organizations.The Telecom, Enforcement, Resource and Monitoring (TERM) Cell established by the DoT was tasked with monitoring compliance with the Circular.Further, non-compliance by the subscriber to the Customer Acquisition Form (CAF) verification requirements would result in disconnection under Clause 9.

A true Copy of the Instructions on Verification of New Mobile Subscribers (pre-paid &Post-paid), File No. 800-09/2010-VAAS dated 09.08.2012 is annexed as **ANNEXURE P-1.**

d. Petitioner No. 1 owns the brand “Paytm”. On 05.04.2013, Petitioner No. 1 obtained the registered its trademark “Paytm”, from the Registrar of Trademarks, Mumbai. The certificate of registration of the Trademark “Paytm” was issued on 22.12.2016 by the Registrar of Trademarks, Mumbai.

A true copy of the certificate of registration of the trademark “Paytm” dated 22.12.2016 issued by the Registrar of Trademarks, Mumbai, is annexed herewith and marked as **“ANNEXURE P- 2”.**

e. On 03.01.2017 the Petitioner No. 2 was granted a license by the RBIunder section 22(1) of the Banking Regulations Act, 1949 to carry on a ‘payments bank business’ in India.

A true copy of the license dated 03.01.2017 granted by the Reserve Bank of India to the Petitioner No. 2 under Section 22(1) of the Banking Regulation Act, 1949 is annexed herewith and marked as **“ANNEXURE P- 3”**

f. 11.10.2017, RBI issued RBI issued the Reserve Bank of India (Issuance and Operation of Prepaid Payment Instruments) Directions, 2017 (hereinafter, ‘RBI Master Direction on PPI, 2017’) under Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007. This Master Direction lays down the eligibility criteria and the conditions of operation for payment system operators, such as the Petitioner No. 2, involved in the issuance of Prepaid Payment Instruments (hereinafter, “PPIs”) in India such as the Paytm Wallet. In particular, it lays down limits on the

monetary amount of the PPI that can be issued, which in turn is dependent on the recorded details ('minimum KYC' oralternatively 'full KYC') of the PPI Holder. For instance, the Paytm Wallet is a semi-closed PPI with a Rs. 10,000 or Rs. 1 lakh limit, dependent on whether the customer has minimum KYC or full KYC. The Master Directions are applicable to all entities approved / authorized by the RBI to operate payment systems involving the issuance of PPIs such as the Petitioner No. 2. As per Clause 9.1 of the Master Direction, a bank or non-bank issuer is permitted to issue PPIs loaded with a maximum amount of Rs. 10,000/- per month, after obtaining minimum details of the PPI holder, also known as 'minimum KYC'. The minimum details include a mobile number verified with One Time Pin (OTP) and a unique identity / identification number of any 'mandatory document' or 'Officially Valid Document' (OVD) listed in the Master Direction on KYC, issued by the RBI from time to time.

g. Once the bank or non-bank entity has completed the KYC of the PPI holder – the full KYC - PPIs of up to Rs. 1,00,000/- each month can be issued to a PPI holder.Further, as per the Master Direction dated 11.10.2017 (amended as on 28.02.2020), the minimum KYC PPI is valid only for a period of 24 months from the date it is issued. For all PPIs issued prior to 28.02.2018, this 24 months-time period is counted from 28.02.2018. That is to say, that all PPIs, including the Paytm Wallet issued prior to 28.02.2018, would only be valid up to 29.02.2020.

A true copy of the Reserve Bank of India (Issuance and Operation of Prepaid Payment Instruments) Directions, 2017 dated 11.10.2017 is annexed herewith as **ANNEXURE P-4.**

h. The Respondent No.2 Authority found that the 2010 Regulatory regime on UCC had not managed to effectively curb the menace of UCC. Hence the 2010 Regulations were superseded by the notification of the TCCCPR 2018 on 19.07.2018, issued by the Respondent No.2 Authority in exercise of its powers under section 36, read with section 11(1)(b) of the TRAI Act, 1997 with the objective of effectively dealing with the nuisance of spam experienced by the subscribers. In this regard, section 11(1)(b) and section 36 of the TRAI Act are reproduced hereunder:

"11. Functions of Authority

[(1) Notwithstanding anything contained in the Indian Telegraph Act, 1885 , the functions of the Authority shall be to -

…

(b) discharge the following functions, namely: -

….

(v) ***lay-down the standards of quality of service to be provided by the service providers and ensure the quality of service*** *and conduct the periodical survey of such service provided by the service providers* ***so as to protect interest of the consumers of telecommunication service****;*

….

(c) levy fees and other charges at such rates and in respect of such services as may be determined by regulations;"

Further, section 36 of the Act of 1997 gives TRAI the power to make regulations. It states:

"36. Power to make regulations

(1) The Authority may, by notification, ***make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.****"*

(Emphasis Supplied)

A True Copy of Telecom Commercial Communications Customer Preference Regulations, 2018 dated 19.07.2018 issued by Respondent No. 2 authority is annexed herewith as **ANNEXURE P-5**

i. The regulatory regime established TCCCPR 2018 has the following salient features:

   i. Complete control to consumers to register their preferences (or lack thereof) for commercial communication (Reg. 6 & 7);

   ii. Mandatory registration of all entities,includingtelemarketers, with the Telcos (referred to in the TCCCPR as 'Access Providers') for sending commercial communication (Reg. 3(1)) and a prohibition on the sending of commercial communication by unregistered entities or UTMs (Reg. 32);

   iii. **Primary Obligation on the Telcos to prevent the sending of UCC**. To this end, the Telcos are mandated to, inter alia:

      a. Register all consumer preferences/modifications in real time (Reg. 12(1))

      b. Register Senders of commercial communication such as telemarketers, principal entities and other intermediaries and carry out robust verification of their identities before such registration (Reg. 5(5), Reg. 12(3));

c. Assign Headers to such registered entities (Reg. 8(3)), and verify the same before such registration, to ensure that such assigned headers are not deceptively similar to those of corporates or well-known brands (Clause 4(1)(b) read with Clause 4(1)(f) of Schedule I);

d. Assign unique Content Templates to such registered entities after verifying the same (Reg. 8(4) read with Clause 4(3) of Schedule I);

e. Ensure that no commercial communication takes place over its networks except by registered entities and through the headers assigned to them (reg.10);

f. Ensure that no commercial communication takes place over its networks except as per the registered preferences of the consumer (Reg. 9); and

g. Ensure that all pre-regulatory checks are carried out for sending any commercial communication (Reg. 13(1));

iv. **Primary obligations on the Telcos to punish/ penalise violations of the TCCCPR by senders**. To this end, the Telcos are mandated to, inter alia:

a Set up robust complaint redressal mechanisms for consumer complaints against UCC (Reg. 23, Reg. 25);

b Detect, identify and act against unregistered sender(s) of commercial communication (Reg. 5(9)); and

c To take immediate remedial action against sender(s) not complying with the regulatory requirements (Reg. 25(4) (for RTMs); Reg. 25(5) & (6) (in case of UTMs).

v. Institute use of Distributed Ledger Technologies (DLT) by Telcos for controlling and managing the UCC ecosystem (Reg. 13), in particular, to ensure that all network related actions are non-repudiable, i.e., identifiable and verifiable (Reg.12)

vi. Obligation on TRAI to initiate inquiries and take action against defaulting Telcos (Regs.21, 27 and 28)

j. Legitimate commercial communication is usually sent bybusiness entities, banks such as the Petitioners to their customers, by engaging the services of a Registered Telemarketer (hereinafter “RTM”). A telemarketer has been defined under regulation 2(bp) of the TCCCPR, 2018 as, *“a person or a legal entity engaged in activity of transmission or delivery of commercial communication or scrubbing or aggregation.”*An example of a registered telemarketer is the company Pinnacle Teleservices Private Limited, which has been engaged by the Petitioners to send out legitimate commercial communication on its behalf to its customers.

An instance of legitimate commercial communication sent using Petitioner No. 1's registered message header "iPaytm" is as follows:

"Paytm never calls asking for OTP. Sharing this gives them full access to your Paytm Wallet. Your confidential login OTP is xxxxx."

An instance of legitimate commercial communication sent using Petitioner No. 2's registered message header "PAYTMB" is as follows,

"Never share your OTP, Debit Card number, ATM PIN, Paytm Password or Passcode with anyone. Do not transfer money for any fake calls for lucky draw or prizes"

It is pertinent to mention that neither the Petitioners, nor their associated companies send messages to its customers regarding completion or conversion of minimum KYC to full KYC. This is a ploy that has been developed by senders of fraudulent & unsolicited commercial communication to dupe innocent customers of various Telcos.

A true copy of a legitimate commercial communication sent by the Petitioner No. 1 & 2 using its registered message headers"IPAYTM " and "PAYTMB" is annexed herewith as **ANNEXURE P-6 (COLLY)**

k. Customers of the Petitioners and its associate companies/ related parties/ group companies have been receiving fraudulent messages from message headers/ content templates deceptively similar to the official headers/ content

templates of the Petitioners and its associate companies/ related parties/ group companies, typically informing them that their Patym account has been suspended and directing them to call a particular number.

True copies of operator wise fraudulent messages received by customers of the Petitioners and its associate companies/ related parties/ group companies from deceptively similar message headers and content templates have been annexed herewith and marked as **"ANNEXURE P - 7".(colly)**

I. The Petitioners and their associate companies/ related parties/ group companies have registered themselves as "principle entities" with some of the Respondent Telcos. After registration as a principle entity, the Telco grants access to an online portal of the Telco where they can upload their message headers and content templates. It is on this online portal that the Principle entity also has to upload its customers preferences.

Some of the registered message headers of the Petitioners and its associate companies/ related parties/ group companies assigned to authorized RTMs are "BPaytm", "FPaytm", "PAYTMB", "ipaytm", "PAYTMC","Vpaytm", "PAYTMM", "iPMall", "lpaytm", "mPaytm", "GMPIND" and "PFGAME

A true copy of a list of all the official message headers of the Petitioners and its associated companies dated NIL registered with the Respondent Telcos are marked as **"ANNEXURE P - 8".**

A true copy of a list of all the official message content templates of the Petitioners and its associate companies/

related parties/ associated companies dated NILregistered with the Respondent Telcosare marked as **"ANNEXURE P - 9".**

True copy of the certificate of registration of the Petitioner No. 1 with Respondent No. 8Telco dated 21.03.2020 as a principle entity has been annexed herewith and marked as **"ANNEXURE P - 10 ".**

True copies of the certificate of registration of the Petitioner No. 2 with Respondent No. 8 Telco dated 04.02.2020 as a principle entity has been annexed herewith and marked as **"ANNEXURE P -11 ".**

True copies of the certificate of registration of the Petitioners' associate companies/ group companies Paytm First Games Private Limited dated and Paytm E-Commerce Private Limited with Respondent No. 8 Telco dated 05.02.2020 and 04.02.2020 and of Paytm Money Limited with Respondent No. 6 dated 02.03.2020 has been annexed herewith and marked as **"ANNEXURE P - 12 " (Colly).**

Mode of UCC/ Fraud

l. It is submitted that despite this regulatory regime, certain fraudulent senders have registered themselves as RTMs and been assigned Headers and content templates by the Respondent Telcos that are deceptively similar to the Petitioners' and its associate companies/ related parties/ group companies' legitimate and authorised Headers/Content Templates, and contain the words "Paytm", "PTM","PYTM" or other deceptive permutations, in order to defraud the Petitioners' customers. In addition to

fraudulent messages, these fraudsters/ spammers also use voice calls as a means of defrauding customers, by misrepresenting themselves as beingemployeesof“Paytm” By way of these deceptive voice calls and messages, fraudsters carry out phishing attacks on the recipients of such fraudulent commercial communication, which is explained below:

a) **Unsolicited Commercial Communication by way of phone calls** is usually from fraudsters pretending to be representatives of the Petitioner No. 2, asking customers to disclose their bank details, “One Time Passwords” and other information, falsely representing that such information is required for the purposes of completion of the KYC, or for the purposes of receiving bogus cash bonuses, lottery amounts, loans, or other investment opportunities. This is one of the methods of duping customers and is also known as voice phishing or “vishing”. Over such a phone call, fraudsters may also ask the recipients of such communication to open a particular webpage or browser by sending them a link, and asking them to fill details on that particular web page. This too has the same effect, and all sensitive information entered on such page is then misused.

b) **Fraudsters also use ‘look-alike’ headers deceptively similar to the Petitioners’ or its associate companies/ related parties/ group companies’ official Message Headers/Sender**

IDs.Some of the reported fraudulent IDs/ headers include IPAYTN, PYTKYC, PTMKYC. Through this method, fraudsters send out mass messages to people, irrespective of whether they are customers of the Petitioners' or not. These headers are only examples of "reported" headers and there are many other such "look alike" headers that are still being used to mislead customers of the Petitioners. Thus, these headers are only a small subset of a larger set of fraudulent headers that are being used for phishing attempts that are not reported.The*modus operandi* of these fraudulent RTMs is described hereinbelow:

(i) **Such fraudulent messages either contain a link or a phone number** on which the recipient of such message is asked to call. The message will typically contain (including but not limited to) details of bogus cash prizes, cash bonuses, investments, or will be a false intimation to the customers that their KYC formalities need to be completed to avoid disruption or restriction in their Paytm wallet services.It is reiterated that neither the Petitioners, nor their associated companies/ related parties/ group companies send messages to its customers regarding completion or conversion of minimum KYC to full KYC. This is a ploy that has been developed and adopted by senders of fraudulent &unsolicited commercial communication to

dupe innocent customers of the Respondent Telcos.

(ii) Upon clicking the link, a **screen recording or mirroring app gets installed** on the recipient's mobile device thereby giving the sender of such fraudulent communication access to all the digits entered for online payments such as the credit/ debit card numbers, CVV number, one-time passwords etc.

(iii) **Alternatively, if the message contains a phone number, and if the recipient of such message calls back, he/ she may be directed to a particular website** or web browser, and asked to enter their bank details while the fraudster remains on call with the customer.

c. Further, **unregistered telemarketers (hereinafter "UTMs") are also responsible for sending bulk fraudulent messages**, however, for this purpose they use phone numbers which are allotted to them without proper verification, in contravention of the DoT SIM verification Circular, 2012

Petitioners' Data and Analysis

m. Fraudulent phishing activities have seen a dramatic rise in the last year, in part due to the RBI amending its Master Direction on PPI, 2017 by a circular dated 30.08.2019, titled 'Amendment to Master Direction on Issuance and Operation of Prepaid Payment Instruments' (hereinafter '2019

Amendment to RBI PPI Master Direction') Vide this amendment the time period for which the minimum KYC PPI would remain valid was extended from a period of 18 months to 24 months. This period of 24 months is counted from the date on which the PPI is issued. However, for PPIs issued prior to 28.02.2018, the minimum KYC would be valid only up to 29.02.2020.Pursuant to this Amendment, there has been a drastic increase in the number of reported fraudulent phone calls and messages (usually regarding the completion of e-KYC formalities) being received by the customers of the Petitioners.

n. Fromthe months of November 2019 to May 2020, nine Telcos including Respondent No. 3 – 9 Telcos have issued 249 Unique SMS headers which have been reported by the customers of the Petitioners as being fraudulent messages. These headers have been reported by customers of the Petitioners to the Petitionersthroughvarious customer interface channels such as Paytm Mobile App, Interactive Voice Response System (IVRS), Emails, Social Media, Customer Care Helplines etc. The prefix of each message header identifies the Telco which issued the said message headers. These fraudulent reported messages were all regarding the conversion of minimum KYC to full KYC, with the senders of these messages hoping to pass these messages off as genuine and legitimate messages sent by the Petitioners' or their associated/ group companies. Despite a significant effort by the Petitioners to spread awareness regarding these fraudulent messages & phone

calls, customers are falling prey to such unsolicited commercial communication. As such, this list of 249 message headers not only includes headers that contain the word “PAYTM” or its derivates, but also those messages sent from headers, which are not necessarily deceptive, but whose content contains the word “PAYTM” or its derivatives.

The customer complainants' phone numbers and identifying details have been supplied to the relevant Telco Respondent in the complaints made to them for action. They have been removed from the present list in the interest of data privacy.

A true copy of a list dated NIL compiled by the Petitioners containing 249 fraudulent headers reported between November 2019 and May 2020 by the customers of the Petitioners and its associate companies/ related parties/ group companies is annexed herewith and marked as **“ANNEXURE P - 13 ”.**

o. On a perusal of the list of 249 headers issued by nine Telcos including the Respondent No. 3 to 9 Telcos, it emerges that the maximum number of fraudulent headers are being issued by Respondent No. 3 BSNL.

This list of 249 headers further reveals that the percentage of fraudulent message headers issued by each of the nine Telcos including the Respondent No. 3 to 9 Telcos is as follows:

Name of Telecom Operator	Number of SenderID/header	Percentage Contribution
BSNL	121	49.8%

QTL	58	22.7%
Vodafone	41	16.1%
Airtel	15	5.9%
MTNL	4	1.6%
VMIPL	4	1.6%
Unrecognized	3	1.2%
Tata	2	0.8%
Jio	1	0.4%
Total	249	NA

The list of 249 message headers issued by the various Telcos including Respondent No. 3 to 9 Telcos can further be categorized into only those headers which contain the word “PAYTM” or its derivatives. From the list of 249 message headers, only 34 headers are deceptively similar to the Petitioners or its associated companies. While the remaining headers may not contain the word “PAYTM” or its derivatives, the message content contains words deceptively similar to “PAYTM” and its derivatives. The customer complainants' phone numbers and identifying details have been supplied to the relevant Telco Respondent in the complaints made to them for action. They have been removed from the present list in the interest of data privacy.

A true copy of a list dated NIL compiled by the Petitioners containing 34 messages headers reported by the customers of the Petitioners and its associate companies/ related parties/ group companies. is annexed herewith and marked as **“ANNEXURE P - 14”.**

q. Over the last few months, the Petitioners have observed that the content template of fraudulent messages, by and large remains the same. Only the deceptively similar keyword i.e. the word “PAYTM” or its derivative, and the phone number, belonging to the fraudster, on which the recipient of the message is asked to call back, vary. It has been observed by the Petitioners, that the phone number of the fraudster remains active only for a few hours or days after which it becomes impossible to trace the user of such phone number. It has been observed that the general content template for fraudulent messages is as follows:

“Your <Paytm Keywords> Has Been Expired. Contact Customer Care No.:-<Fraudster number> Immediately. Your account will Block within 24 hrs”

The Petitioners have collated a list of 234 fraudulent messages with identical content template, sent using message headers that are not deceptively similar to the official headers of the Petitioners and/or its associate companies/ related parties/ group companies. The customer complainants' phone numbers and identifying details have been supplied to the relevant Telco Respondent in the complaints made to them for action. They have been removed from the present list in the interest of data privacy.

A true copy of a list dated NIL containing 234 fraudulent messages with an identical content template reported by the customers of the Petitioners and its associate companies/

related parties/ group companies has been annexed herewith and marked as **"ANNEXURE P - 15 ".**

With regard to reported fraudulent phone numbers, between September 2019 to May 2020, customers of the Petitioners and its associated companies have reported 5407 numbers from which they have received fraudulent phone calls attempting to defraud the recipients of the fraudulent commercial communication, at the **first instance**. The Petitioners have been diligently reporting these fraudulent phone numbers to the Respondent No. 3 to 9 Telcos, however so far only about 550 phone numbers have been blocked, the maximum arebeing blocked by Respondent No. 5 Vodafone, while most of the other phone numbers remain unblocked. Out of the 5407 phone numbers, customers have reported fraudulent phone calls received by them at the**second instance** by 296 (out of the 5407phone numbers), and received by them at the **third instance** by 50 (out of the 296 phone numbers). The customer complainants' phone numbers and identifying details have been supplied to the relevant Telco Respondent in the complaints made to them for action. They have been removed from the present list in the interest of data privacy.

A true copy of a list dated NIL of the 5407 compiled by the Petitioners from which fraudulent phone calls were reported by the customers of the Petitioners and its associate companies/ related parties/ group companies at the first instance between September 2019 to May 2020 is annexed herewith and marked as **"ANNEXURE P - 16".**

A true copy of a list dated NIL compiled by the Petitioners containing 296 fraudulent phone numbers reported by the customers of the Petitioners and its associate companies/ related parties/ group companies at the second instance is annexed herewith and marked as **"ANNEXURE P - 17".**

A true copy of a list dated NIL compiled by the Petitioners of the 50 reported fraudulent phone numbers reported by the customers of the Petitioners and its associate companies/ related parties/ group companies at the third instance is annexed herewith and marked as **"ANNEXURE P - 18 ".**

u. It is further observed that since 19th September, 2019, an average 26 fraudulent phone numbers have been reported on a daily basis by the Petitioners' customers to the Petitioners' customer care portals. As such, thesefiguresonly represent the reported phone numbers and thereare a large number of phone numbers through which fraud has been originated which remain unreported.

v. The difference between minimum KYC PPI and the complete/ full KYC PPI was clarified vide circular no. DPSS.CO.PD.No.1198/02.14.006/2019-20 dated 24.12.2019 issued by the RBI. As per clause 2 (f) minimum KYC PPI can only be used for purchase of goods and services and not for fund transfers. That is to say, the Paytm Wallet can only be used for 'Merchant to Merchant' and 'Person to Merchant' transactions on completion of the minimum KYC requirements, whereas completing the full KYC, in addition to many other benefits, also gives PPI

holders, in this case are Paytm Wallet holders, the benefit of 'Person to Person' transactions as well as a higher monthly limit of Rs. 1,00,000/- that can be loaded on to the PPI i.e. the Paytm wallet.

A true copy of circular no. DPSS CO.PD.No.1198/02.14.006/2019-20 dated 24.12.2019 issued by the RBI is annexed herewith and marked as **"ANNEXURE P-19"**

v. Despite the TCCCPR having been issued in 2018, the Respondent No. 2 Authority issued a direction dated 20.01.2020 under section 13 of the TRAI Act, 1997, acknowledging the lack of implementation of the TCCCPR 2018 by access providers and directing full implementation of the same. In particular, it was stated:

> *"11. And whereas after having various meetings with Access Providers, it is observed that: -*
>
> *a) no significant progress has been shown by Access Providers for migration of existing headers and consents with principal entities to DLT system of Access Providers;*
>
> *b) out of approximately 9 lakh unique headers existing in market, as per the information submitted by Access Providers, so far negligible number of headers have been registered by Principal Entities;*
>
> *c) many principal entities across all Access Providers are not fully aware about the requirements and steps of registration of entity, header, consent etc;*
>
> *12. Now, therefore, the Authority, in exercise of the powers conferred upon it under section 13, read with sub-clauses (i)and (v)of clause (b) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act, 1997 (24 of 3 1997), and the provisions of the Telecom Commercial Communications Customer*

Preference Regulations, 2018, ***hereby directs all Access Providers to:*** -

a) ***not assign new SMS and voice headers without registration in the new system established by Access Providers in accordance with the regulations****;*

b) ***migrate the existing SMS and voice headers as listed by the Authority, based on the lists of headers submitted by Access Providers*** *(consolidated list shared by TRAIwith Access Providers vide email dated 9th January, 2020, as provided in Annexure-I), and which are in use in last one year, to new system within four weeks' time;*

c) *ensure that Principal Entities submit list of existing subscriber's consent to Access Providers within fifteen days from the issue of this Direction;*

d) *ensure that consents recorded prior to six months from the date of issue of this Direction, become invalid, and should not be migrated to the new system;*

e) *ensure that all new consents of subscribers shall be registered in the new system, as per provisions of the regulations;*

f) *ensure that Principal Entities are not able to send promotional messages or calls to the subscribers who have not opted for such preference, if they have not shared subscribers' consent with Access Providers or not acquired consent from the subscribers according to the provisions of the regulations;*

g) ***ensure that Principal Entities are not able to send any commercial communication till they register themselves with Access Providers****;*

h) *ensure that Principal Entities are not able to send any service and transactional messages till they register content template against specific registered header with Access Providers"*

(Emphasis Supplied)

A true copy of the direction dated 20.01.2020 issued by Respondent No. 2Authority is annexed herewith and marked as **"ANNEXURE P- 20 ".**

w. The Petitioner has been pro-active to protect its customers from fraudulent activity. The Petitioner No. 2 have been complying with the various circulars issued by RBI from time to time which require a bank to formulate a grievance redressal mechanism for its customers, and also publicize the same. .Additionally, the Petitioner No. 2 also has duly implemented the necessary measures in compliance with RBI directives, circulars and guidelines pertaining to Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds and Cyber Security Framework in Payments Banks.

x. Further, on its part, the Petitioners has been taking major countermeasures to safeguard user accounts including the use of the latest cybersecurity tools. This new feature analyses installation of screen sharing applications on the user devices which might trigger fraudulent transactions and advises users to uninstall them. A typical notification alert sent on the Paytm App to their customers reads as follows:

"Security Alert!

Your Phone has following apps that can record your screen and steal your confidential data:

<Name of the screen sharing app>

Due to security risk, Paytm will not start until such apps are uninstalled."

The Petitioners are also leveraging Artificial Intelligence to instantly detect suspicious transactions. Depending on the identified threat level of a transaction, the Artificial Intelligence either slows it down or completely blocks the payment from getting completed. The Artificial Intelligence has been specifically designed keeping in mind the patterns of the various fraudulent communications being run by fraudsters and is, therefore, able to combat most attacks on user accounts in real-time.

A true copy of the notification alert sent on the Paytm when it detects a screen recording application on the mobile device is annexed herewith and marked as **"ANNEXURE P- 21"**

x. In conformity with the various RBI circulars on customer protection,some of the other features introduced by the Petitioners on the "Paytm" app, so as to mitigate online frauds, include:

(i) **Screen blackout functionality:** Screen blackout functionality ensures that all sensitive screens get blacked out so that fraudster is not able to see anything on his device screen and hence cannot carry on with the fraud.

(ii) **Blocking usage in case any Remote Access app is installed:** As mentioned above, the Paytm app has also released a feature in its latest version of apps, which would block usage of the Paytm app, in case it

is able to detect that any remote access apps are also installed along with on the device.

(iii) **Fraud prevention engine –** The Paytm App's Risk Engine detects suspicious transactions and blocks them in real time. Risk Engine works on multiple rules configured based on velocity variables, customer profiles, pattern of transactions.

(iv) **Two factor authentication:** A Paytm Appuser needs both password and OTP (which is sent to the user's registered mobile number) every time for logging into account on a new device. This is to mitigate situation where if the fraudster acquires password somehow, he would need OTP also for logging into user's Paytm account.

(v) **Applock:**This is an additional layer of security. User can allow pattern lock/touch ID/face ID (depending on the device). When activated, User would need to unlock Applock in order to access savings passbook and pay/send money.

(vi) **Bank Passcode:**Paytm Payments Bank savings account is also safeguarded by a 4-digit passcode.

y. As per the RBI annual reports for the financial years 2017-18 and 2018-19, the cumulative figures for bank fraud are as follows:

Financial Year	Amount lost in bank fraud

	(INR in millions)
2017-18	411,670
2018-19	715,429

These are the figures of cumulative bank fraud as a result of phishing activities, as well as forgery, cheating etc. There has been a drastic increase in bank fraud from 2017-18 to 2018-19, with an approx. 60% increase in the amount of money lost to bank fraud. It is pertinent to mention that the cumulative amount lost by the customers of the PetitionerNo. 2 alone because of phishing activities is about Rs. 10 crores (Rs. 100 million approx) through the months of July ’19 to April ’20.

A true copy of the RBI annual report dated NIL for the financial year 2018-2019 has been annexed herewith and marked as **“ANNEXURE P- 22”.**

y. On 20.01.2020 the Petitioner No. 2 addressed a representation to Shri Ajay Kumar Bhalla, Secretary, Ministry of Home Affairs notifying the Ministry of the increasing fraudulent activity with illustrations of the same,and contained suggestions on mitigating measures to prevent cyber-crimes and financial frauds. In particular, it was stated:

“*a. Develop/enhance framework for addressing financial frauds propagating through use of telecom operator services.*

…

Define procedure at SHO level for accepting such complaints:

- *On receiving complaints from financial institutions:*
  - *SHO may intimate telecom operator for immediate blocking of number and inform MHA cyber security cell for further action.*
- *From individuals:*
  - *On receiving complaints from individuals, the concerned financial institution is informed for further investigation and blocking of account after due verification*
  - *inform MHA cyber security cell is informed for further action.*

….

iii. ***Close co-ordination with other govt. agencies like CERTin and TRAI***

With MHA being the agency for enforcing preventive and corrective measures for internal security, CERTinas the nodal agency for responding to computer security incidents and TRAI being the authority for telecom services, close co-ordination can ensure better preparedness and response to such frauds. A specific and action oriented framework among the aforementioned agencies on dealing with such frauds emanating from using telecom services is requested be defined , with identification of standard operating procedures for authorities in accepting fraud complaints & ensuring near real time corrective measures."

A true copy of the letter dated 20.01.2020 addressed to the Secretary, Ministry of Home Affairs by the Petitioner No. 2, is annexed herewith and marked as **"ANNEXURE P-23".**

z. On 20.01.2020, a representation was also sent by the Petitioner No. 2 Bank to the Director General of the Indian Computer Emergency Response Team (hereinafter "CERT-IN") requesting them to take action against fraudulent commercial communication. In particular, this letter sought collaboration of CERT-IN with MHA & TRAI on defining the process and framework to deal with such telecom frauds.The letter, in part recommended:

> *"4. Basis our relevant experience and learnings from specificfraud patterns and scenarios, with due respect,*
>
> *i.* ***Further increase focus on frauds propagating through telecom services especially related to Banking and Finance industry***
>
> ***..***
>
> ***ii. Collaborate with MHA & TRAI on defining the process and framework to deal with such telecom frauds***
>
> ***With CERT-In as the nodal agency for responding to computer security incidents, MHA being responsible for enforcing preventive & corrective measures and Telecom Regulatory Authority of India (TRAI) being the authority to regulate telecom services; close co-ordination can ensure better preparedness and response to such frauds. A 'specific & action oriented' framework among the aforementioned agencies on dealing with such frauds emanating from using telecom services is requested be defined****, with identification of standard operating procedures for authorities in accepting fraud complaints & ensuring near real time corrective measures.*
>
> ***iii. Telecom fraud incident analysis and pattern identification***
>
> *Since fraudsters are generally using a certain modus operandi for propagating frauds, there is a need to identify patterns being used by fraudsters using SMS message formats, calling customers for undertaking eKYC etc. CERT-In may choose to issue telecom fraud related specific measures with other relevant*

Ministries/ Organizations like Ministry of Home Affairs (MHA), Ministry of Finance (MoF), Reserve Bank of India (RBI), Ministry of Electronics and Information Technology (MeitY), Department of Telecommunications (DoT), Telecom Regulatory Authority of India (TRAI), Ministry of Consumer Affairs (MCA) as well as Banking and Financial Services industry for them to take further action and preventive measures.

iv. Advisory release on structural frauds using telecom operators

v. Spread awareness among customers and merchants

While PBBL has been continuously running campaign to spread awareness regarding frauds propagating through telecom services by running campaigns, promotion on social media, there is a requirement for a co-ordinated effort between all stakeholders to spread awareness among customers, merchants regarding do's, and don'ts while making or receiving digital payments."

However, no response to the same has been received yet by the Petitioner No.2 from CERT-IN.

A true copy of the letter dated 20.01.2020 addressed to the Director General, Indian Computer Emergency Response Team (Cert-IN) under the Ministry of Electronics and Information Technology is annexed herewith and marked as **"ANNEXURE P- 24 ".**

aa. On 21.01.2020 a representation was sent by the Petitioner No. 2to the Respondent No. 2 authority, in which certain measures were proposed to prevent financial frauds propagating through use of telecom services. The representation also enclosed a list of 6000 fraudulent cases with mobile numbers that had been used to send fake messages to its customers, and sought blocking of the said

numbersand re-iterated the suggestions made to the MHA and CERT-In in the 20.01.2020 letters. The Petitioner No. 2 also made some additional recommendations to the Respondent No. 2 such as:

" …

(i) ***Stringent Agency/ KYB onboarding and process to source of fraudulent messages:*** *Telecom operators who sell bulk messaging service to agencies who may further sell them to sub-agents should follow well defined stringent Know Your Business (KYB) process which should be made applicable to all telecom operators as well as re-sellers. This should include detailed on-boarding process, requirement of proper documentation etc. On non-adherence to the processes, there may be stringent penal measures. Telecom operators must be required to allow traceability of source of fraudulent bulk SMSs so that the real companies/organizations/individuals propagating fraud can be identified and brought to justice.*

(ii) ***Mandatory Content Review Process on Bulk Messages:*** *Telecom operators and resellers must be obligatorily required to review content of bulk messages. TRAI may require such a restriction to be in effect, may be above a certain threshold of messages say 500 messages a day.*

Telcos may be asked to have adaptive SMS Filtering platform that dynamically parses the SMS content on the basis of identified key words and on the basis of match grades the message as per risks as High, Medium, Low and no risk categories. In case of High and medium risk category messages, SMS may be delivered with warning on 'top' of the message.

(iii) ***Real time blocking of numbers propagating fraud***

….

There is an urgent need of creating a process whereby financial institutions after due verification can report numbers through which fraud messages are being propagated, and then in real time the mentioned numbers can be blocked by telecom

operators. We believe, the way digitization has improved the speed and ease of money, we must safeguard our customer interests with an equally fast and rapid response.

(iv) ***Short codes matching names of financial institutions to be restricted for use:*** *Fraudsters increasingly use short codes, which have names similar to genuine financial institutions to trick innocent citizens into revealing bank account related details. For e.g. A fraudster can send a message to a Paytm user from BPAYTM or DPAYTM short user code etc., which makes a customer believe that the message is genuine.*

……..

Also,telecom operators and resellers must maintain a common registry of short codes issued so that once a short code is issued to an entity by a telecom operator, it must not be issued to any other entity for a given period. Similar to domain names, uniqueness and disambiguation at the level of creation would restrict the ability of fraudsters to convince gullible people and defraud them.

(v) ***Close coordination with other Government agencies like MHA and CERTin:****With Telecom Regulatory Authority of India(TRAI) being the authority to regulate telecom services, MHA being responsible for enforcing preventive and corrective measures for internal security, CERTinas the nodal agency for responding to computer security incidents; close co-ordination can ensure better preparedness and response to such frauds. A 'specific and action oriented' framework among the aforementioned agencies on dealing with such frauds emanating from using telecom services is requested be defined, with identification of standard operating procedures for authorities in accepting fraud complaints & ensuring near real time corrective measures.*

5. *We believe that the above measures will go a long way in stopping fraudulent messages.* ***Further, we are also enclosing a list of 6000 fraudulent cases along with mobile numbers that have been used to send fake messages to customers (enclosed at Annexure 1). We request that these numbers be blockedat the***

***earliest**. We shall be happy to provide any additional information in this regard."*

However, no response to this representation has been received by the Petitioner No. 2 from the Respondent No. 2 Authority.

A true copy of the letter dated 21.01.2020 addressed to the Chairman, of the Respondent No. 2 authority by the Petitioner No. 2 is annexed herewith and marked as **"ANNEXURE P- 25 ".**

bb. The Petitioner No. 2 also sent e-mails dated 23.01.2020 to the Respondents Nos. 5, 6 and 7 Telcos reporting the deceptive look-alike headers employed to defraud the Petitioners' customers. In the said emails, the Petitioner No. 2 enclosed a list of fraudulent message headers and phone numbers which the customers of the Petitioners and its associate/ group companies has reported to the Petitioners as being fraudulent, requested that these message headers and phone numbers be blocked.

True Copies of the e-mails dated 23.01.2020 sent by the Petitioner No. 2 to the Respondents Nos. 5, 6 & 7Telcos are annexed collectively as **ANNEXURE P-26 (colly)**

cc. On 24.01.2020 the Petitioner No. 2 filed a Complaint with the SHO, Cyber Crime Cell, Gautam Budh Nagar, Uttar Pradesh, requesting for registration of an FIR against unknown persons for committing serious offences of

misrepresentation, cheating, criminal breach of trust, fraud, wilfully and in collusion with each other against the public at large and the customers of the Petitioner, thereby causing wrongful gain to themselves and wrongful loss to the Petitioners and its customers. Along with the complaint, a list of the phone numbers of 3500 fraudsters was annexed for action to be taken against them.

A true copy of the complaint dated 24.01.2020filed by the Petitioner No. 2to the Station House Officer, Cyber Crime Cell, GautamBudh Nagar, Uttar Pradesh against “unknown persons” is annexed herewith and marked as **“ANNEXURE P-27”.**

dd. A letter dated 29.01.2020 was sent by the Petitioner No. 2 to the Respondent No. 1 Department of Telecommunications (“DoT”) with similar content to the21.01.2020 representation made to TRAI,apprising the DoT of the financial frauds taking place. Lists of codes and numbers being used to propagate the fraud were enclosed, and the DoT was requested that the same be blocked at the earliest. However, no response to this representation has been received by the Petitioner No. 2 from the Department of Telecommunications,nordoes it appear that any action has been taken by them till the date of filing the present petition.

A true copy of the letter dated 29.01.2020 sent by the Petitioner No. 2, to the Deputy Director General, Department of Telecommunications (“DOT”), is annexed herewith and marked as **ANNEXURE P- 28**.

ee. On 30.01.2020 the Petitioner No. 2 sent a reminder of its 23.01.2020 e-mail to the Respondents Nos. 5 and 7Telcos, requesting that appropriate action be taken against the reported headers and short codes.

True Copies of e-mails dated 30.01.2020 sent by the Petitioner No. 2 to the Respondents Nos. 5 & 7Telcos is annexed as **ANNEXURE P-29 (Colly).**

ff. On 31.01.2020 the Petitioner No. 2 received a Reply to its e-mail dated 23.01.2020, by the Respondent No. 7 Telco, i.e. RelianceJiowhich informed it of the Respondent No. 7's view that the scope of action against fraudulent UCC under the TCCCPR does not extend to unilateral blocking of access to telecom services unless so directed specifically by telecom and law-enforcement authorities.

True Copy of e-mail dated 31.01.2020 sent by the Respondent No.7 to the Petitioner No. 2 is annexed as **ANNEXURE P- 30.**

gg. On 03.02.2020 the Petitioner No. 2 issued letters to Respondent Nos. 3, 5, 6, 7, and 8 Telcos, requesting them to block sender IDs that were deceptively similar to or containing the words "Paytm" and "Pytm", and phone numbers from which fraudulentcommunicationwas being sent to the Petitioners' customers.

True copies of the letters dated 03.02.2020 sent by the Petitioner No. 2 to the Respondent Nos. 3 and 5-8 telcos,are annexed collectively herewith as **ANNEXURE P-31 (COLLY).**

hh. On 05.02.2020, an FIR was registered at Kavi Nagar Police Station, Ghaziabad, U.P. by an aggrieved customer of the Petitioner No. 2 who had fallen prey to phishing activities, under section 420 of the Indian Penal Code, 1860 & Section 66D of the Information Technology Act, 2000. This FIR was filed against the Petitioner No. 2, its founder Mr. Vijay Shekhar Sharma and Senior Vice President of Petitioner No. 1 Mr. Ajay Sharma.SimilarFIRsare being filed against the Petitioners and its officials by aggrieved customers of the petitioner No. 2 who have lost large sums of money under the misconception that it is the Petitioners that can prevent/ halt the fraudsters rather than the Respondent Telcos..

A true copy of the FIR dated 05.02.2020 with its true translated copyhave been annexed herewith and marked as **“ANNEXURE P- 32 (Colly) ”.**

ii. On 12.02.2020, the Petitioner No. 2 and its officials filed Writ Petition (Criminal) No. 2879 of 2020before the Hon’ble High Court of Judicature at Allahabad seeking the quashing of the FIR dated 05.02.2020.

jj. On 12.02.2020, the Petitioner No. 2 received an email response to is representation dated 20.01.2020 from the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, stating that in order to curb financial frauds, companies (such as the Petitioners) issuing PPIs though wallets and through mobile apps must explore the possibility of modifying their apps in a manner, so as to prevent installation of fraudulent screen sharing apps on the

customers' device, and to store the metadata/ data logs so as to aid the investigation of fraudulent activity.

A true copy of the email dated 12.02.2020 sent to the Petitioner No. 2 by the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs is annexed herewith and marked as **"ANNEXURE P- 33".**

kk. On 14.02.2020 the Petitioner No. 2 received a 'Meeting Notice' from the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, stating that a meeting had been held on 13.02.2020 under the chairmanship of the Joint Secretary, Cyber & Information Security Department, Ministry of Home Affairs, to discuss the best possible approach to be adopted and means and measure to prevent/ minimize financial fraud. Vide this letter dated 14.02.2020 the Petitioner No. 2 was invited to participate in a meeting on 19.02.2020, of the working group, on creating a working document on integration of the cyber-crime portal with payment intermediaries.

A True Copy of the letter dated 14.02.2020 from the Indian Cyber Crime Coordination Center, Ministry of Home Affairs to the Petitioner No. 2 is annexed herewith and marked as**"ANNEXURE P- 34".**

ll. On 17.02.2020, the Petitioner No. 2 received an email from theIndian Cyber Crime Coordination Center,MHA, requesting the Petitioner No. 2for details of their customer care officials, official headers used by the Petitioners and its associated companies to send legitimate bulk commercial

communication to customers and material prepared by the Petitioners on customer awareness. In this regard, the email stated,

> *"As discussed in the meeting held on 13.02.2020, another meeting has already been scheduled on 19.02.2020 and it was already requested vide our mail under reference to share the following information with I4C:*
>
> *"1. Details of your help desk/ customer care number and Nodal Officer (Name & Designation, mobile number, official phone number, email ID etc.)*
>
> *2. Details of your valid bulk SMS headers*
>
> *3. Please share your awareness material regarding financial frauds such as audio, video, pictorial etc.*
>
> *4. Details of FAQ regarding your mobile app for helping citizens*
>
> *5. Suggestions/ comments to be discussed in the next meeting"*

A true copy of the email dated 17.02.2020 from the Indian Cyber Crime Coordination Center, Ministry of Home Affairs to the Petitioner No. 1 is annexed herewith and marked as **"ANNEXURE P- 35 ".**

mm. Vide Order dated 18.02.2020 passed in W.P (Crl.) 2879/2020 the Hon'ble High Court of Judicature at Allahabad issued notice to the Respondent Complainant. The matter was listed for 18.03.2020, however no other orders have been passed till date.

True Copy of Order dated 18.02.2020 passed by the Hon'ble High Court of Judicature at Allahabad in W.P (Crl.) 2879/2020 is annexed as "**ANNEXURE P-36"**

nn. Pursuant to the meeting held by Indian Cyber Crime Coordination Center, Ministry of Home Affairs on

19.02.2020, on 27.02.2020 the Petitioner No. 2 submitted a document titled "*Key asks from Stakeholders for Prevention of Financial Frauds through Telecom Services*". In this document, the Petitioner No. 2 put forth its recommendations/ demands from Respondent Nos. 1 and 2, the MHA, Cert-In as well as the Telcos.

A true copy of the document dated 27.02.2020 &titled "*Key asks from Stakeholders for Prevention of Financial Frauds through Telecom Services*" sent by Petitioner No. 2 to the Ministry of Home Affairs, is annexed herewith and marked as **"ANNEXURE P – 37 ."**

oo. On 27.02.2020, a news article was published by *Livemint*titled "*Telcos not doing enough to counter online frauds: Paytm"* regarding the failure of the Telcos to take preventive and punitive measures to curb fraudulent activities over its networks. The news report also highlighted the steps that the Petitioners had been taking, in terms of developing their Artificial Intelligence, coordination with various departments of the government etc. in order to curb the menace of online frauds.

A true copy of the news report dated 27.02.2020 published by Livemintitled "*Telcos not doing enough to counter online frauds: Paytm"* is annexed herewith and marked as **"ANNEXURE P- 38".**

pp. Due to the lack of effective action by the Respondent Telcos, on 28.02.2020 the Petitioner No. 2 sent legal notices to Respondent Nos. 3, 5 and 8 Telcos, calling upon them to

blacklist the telemarketers/ aggregator/ intermediaries sending or responsible for fraudulent messages being sent and to deactivate the mobile numbers being used by fraudsters, in furtherance of its previous communications dated 23.01.2020 and 03.02.2020.The said Legal Notices called upon the Respondent to, ensure inter alia:

> *"…*
> *(vi) Blacklisting of telemarketers using fraudulent headers under Regulation 25 (c) of TCCCPR, 2018. Non-registration of sender IDs deceptively similar to Paytm/Paytm Payments Bank.*
> *(vii) Blocking delivery of SMS having Paytm (or similar keywords) by Fake Headers. Scan filter and block delivery of bulk SMS having the following keywords; "Paytm" & "KYC", "PYTM" & "KYC", "PY2TM" & "KYC", which are not official headers/ short codes.*
> *(viii) Whitelisting of official headers from Paytm companies, which were as follows- "Bsmart", "BPaytm", "Tanla", "FPaytm", "Gupshup", "ipaytm", "Vfirst", "PAYTMB", "Pinnacle", "PAYTMC", "Karix", "Vpaytm", "PAYTMM", "iPMall", "lpaytm", "mPaytm", "GMPIND" and "PFGAME".*
> *(ix) Deactivation of mobile numbers of reported fraudsters shared vide email dated 23rd January, 2020 with immediate effect.*
> *(x) Refrain from activating mobile numbers without following proper process"*

True Copies of the Legal Notices dated 28.02.2020 sent by the Petitioner No. 2 to Respondent Nos. 3, 5 and 8 Telcos are annexed collectively as **ANNEXURE P-39 (colly).**

oo. On 02.03.2020, the Petitioner No. 2 yet again, sent emails to Respondents Nos. 3 – 6 reporting that its customers had reported receipt of UCC in violation of TCCCPR. All relevant

details of such UCC was provided in compliance with Regulation 25(6)(A) of the TCCCPR, 2018, including "first instance", "second instance" and "third instance" violations by Senders, as per complaints received. The said e-mails stated:

> *"Dear Sir/Madam,*
>
> *As per THE TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCE REGULATIONS, 2018 (6 of 2018) dated 19th July,2018, reference point number 23, 1 (b), Our esteemed customers have reported the Commercial communication (Call / SMS). Our customers have reported such communication to your customer service channel. In compliance to section 25 (6) A, the We hereby share the complaint along with First instance, Second Instance and Third Instance list of violation by Senders, as per complaints reported to us. We request for TRAI prescribed action to Sender agencies. We have provided comprehensive complainant, Victim and complaint details, Please let us know if any further information needed from our side"*

True Copies of the e-mails dated 02.03.2020 from the Petitioner No. 2 to Respondents Nos. 3 – 6 Telcos are annexed collectively as **ANNEXURE P-40 (colly.)**

pp. On 20.03.2020 the Petitioner No. 2 filed a complaint with the Superintendent of Police, Cyber Crime, Central Bureau of Investigation against fraudsters, telemarketers and aggregators for the offences of cheating, criminal conspiracy, defamation & defrauding the public.

A true copy of the complaint dated 20.03.2020 filed with the Central Bureau of Investigation by the Petitioner No. 2 is annexed herewith and marked as **"ANNEXURE P-41".**

aq.On 27.03.2020, in response to an email request sent by Petitioner No. 2 for blocking of fraudulent reported headers, Respondent No. 6 responded saying that it could not investigate of the fraudulent headers and phone numbers, with a suggestion that complaints be filed by Petitioner No. 2 with the relevant law enforcement agencies. In this regard, Respondent No. 6's response dated 27.03.2020 was as follows:

> "*Dear paytm team*
>
> *For point number 2 (calls from mobile numbers) – as explained in the call between our CIO and your CEO,* ***we are not an investigating agency; hence any expectation that we will investigate anything related to these numbers is misplaced. As suggested on the call, PayTM should file a complaint with the relevant law enforcement agencies, based on their direction we will be authorised to take action****.*
>
> *…."*

(Emphasis Supplied)

A true copy of the email dated 27.03.2020 sent by Respondent No. 6 to Petitioner No. 2 is annexed herewith and marked as **"ANNEXURE P - 42".**

ar.On 28.03.2020, the Petitioner No. 2 filed a complaint filed a complaint with the Dy. Commissioner of Police, Sector – 6, Noida against five aggregator entities responsible for fraudulent headers, deceptively similar to the Petitioners and their associate companies/ related parties/ group companies being allotted, which contain the words "Paytm", "PTM" or "Pytm", or derivative thereof stating, in relevant part:

> "*Therefore, in light of the aforesaid facts and at the time of such rampant increase in frauds involving the name of our company, we solicit your help to ensure that our trust and faith in law is reinforced and strict*

action is taken against such unknown perpetrators, telemarketer, Telecom Service Providers. They have wilfully, dishonestly, fraudulently and with malafide intention have committed the offences of cheating, criminal breach of trust, fraud, to cause wrongful gain to themselves and cause wrongful loss to innocent people.

Thus, we request your goodself's to register a Complaint under Sections 415, 418, 406, 417, 419,420, 426, 468, 469, 499 and 120-B of the Indian Penal Code, 1860 and Section 66 of the IT Act and other applicable laws against the aggregators listed out in this complaint and other unknown persons who may be involved in this racket and conduct a proper investigation to nab all such culprits involved in it"

A true copy of the complaint dated 28.03.2020 filed by the Petitioner No. 2 with the DCP, Sector – 6, Noida, is annexed herewith and marked as **"ANNEXURE P-43"**

ss. On 30.03.2020, a legal notice was addressed to Respondent Nos. 3 and 4, as a reminder, due to lack of a corrective action from the said Respondents to the emails dated 23.01.2020, request letter dated 03.02.2020 and the legal notice dated 28.02.2020. Along with this legal notice, a list of reported headers with the content of the messages was annexed for reference of Respondent Nos. 3 & 4.

A true copy of the legal notice dated 30.03.2020 sent by Petitioner No. 2 to Respondent No. 3 & 4 has been annexed herewith and marked as **"ANNEXURE P -44 (Colly)."**

tt. The Petitioners have, since January 2020 also been in constant communication with the Respondent Telcos, reporting fraudulent message headers/ short codes and

mobile phone numbers. The Respondent Telcosin some instances have responded to the reports of the Petitioners, however these are ad hoc post facto responses, which suffer from a number of lacunae:

(i) The UCC fraud reported to the Petitioners is a small proportion of the total UCC fraud customers suffer.

(ii) Such action, even when taken by the Respondents is ex post facto or after the fraud or fraud attempt has taken place

(iii) The obligation to prevent such UCC fraud under the TCCCPR is on the respondents. They do not however:

a. Verify RTMs adequately

b. Verify that the entities to whom deceptive Headers or SMS content are issued are in fact authorised by the Petitioners or its associate companies/ related parties/ group companies.

c. Systematically penalise the RTM or UTM instead of merely blocking content in an ad hoc manner

Therefore, a large percentage of the same continue to remain active and defraud the customers of Petitioners and its associate companies/ related parties/ group companies.

True Copies of the Petitioner's e-mail correspondence with Respondent No.3 BSNL are annexed collectively as **ANNEXURE P- 45 (colly).**

True Copies of the Petitioner's e-mail correspondence with Respondent No.4 Quadrant Televentures Ltd. are annexed collectively as **ANNEXURE P- 46 (colly)**

True Copies of the Petitioner's e-mail correspondence with Respondent No.5 Vodafone Idea Limited are annexed collectively as **ANNEXURE P- 47 (colly)**

True Copies of the Petitioner's e-mail correspondence with Respondent No.6 Bharti Airtel Limited are annexed collectively as **ANNEXURE P- 48 (colly)**

True Copies of the Petitioner's e-mail correspondence with Respondent No.7 Reliance JioInfoCom Limited are annexed collectively as **ANNEXURE P-49 (colly)**

True Copies of the Petitioner's e-mail correspondence with Respondent No.8 MTNL are annexed collectively as **ANNEXURE P- 50 (colly)**

True Copies of the Petitioner's e-mail correspondence with Respondent No.9VMIPL are annexed collectively as **ANNEXURE P- 51(colly)**

uu. As per the Petitioner No. 2's records from July 2019 to April 2020, customers of the Petitioner No. 2 alone have lost about Rs. 10 crores (approx). The month wise breakdown of the cumulative sums of money lost by the customers of the Petitioner No. 2 due to phishing frauds is as follows:

Month	**Case Count**	**Amount Lost (In Rupees)**
July 2019	572	69,986.70

Aug. 2019	179	9,49,757.48
Sept. 2019	243	14,67,858.93
Oct. 2019	289	17,15,422.45
Nov. 2019	721	89,51,282.21
Dec. 2019	823	1,01,36,089.87
Jan. 2019	2247	3,07,44,581.29
Feb. 2020	1708	2,01,76,223.25
March 2020	762	1,18,17,535.19
April 2020	820	1,76,02,679.91
Total	**7849**	**10,38,31,417.3**

vv. With the outbreak of the Covid-19 pandemic there has also been a proportionate increase in unsolicited fraudulent communication, which, apart from the usual methods, is also now being sent by persons fraudulently claiming to be 'Corona Relief' funds. There have been multiple media reports highlighting the increase in fraudulent activity in which senders of UCC are luring customers in novel ways into opening emails, text messages and entertaining calls about COVID-19, loans offered during the lockdown period, sale of medical equipment etc.

True Copies of news articles dated18.03.2020, 26.03.2020, 30.03.2020, 02.04.2020, 30.04.2020, 04.05.2020 & 14.05.2020are annexed herewith and marked as **"ANNEXURE P- 52(colly). -**

Conservative estimates of the Respondent No. 2 authority itself suggest that as on December 2019, there were about 982

million (approx. 98.2 crore) mobile phone user in India (including non-smart phone users).The Paytm App alone has a customer base of about 30 crore users, far more than any other Payments App such as Google Pay and Phone Pe which reportedly have a customer base of about 6.7 crores and 18.5 crores respectively. This means that every third mobile phone user is also a user of the Petitioners' services. There have been several instances where fraudsters have sent fraudulent & unsolicited commercial communication, using deceptively similar headers and content to the Petitioners or its associate companies/ related parties/ group companies, to customers who are not users of the services of the Petitioners. The fraudsters target a large number of mobile phone users irrespective of whether or not they are customers of the Petitioners (or their associate companies/ group companies), in the hope that there will be a high "hit ratio" in response to the fraudulent commercial communication.

ww. On 21.04.2020 an article was published on the website www.moneylife.com by one Mr. Yogesh Sapkale stating that the Respondent No. 2 TRAI had refused to give him a concrete answer when he approached them with an RTI application regarding the issue of telemarketers, spammers and senders of fraudulent unsolicited commercial communication. According to the article, Mr. Sapkale's RTI query had specifically sought the following information, in response to which he was directed to the link totheTCCCPR2018 on the TRAI website. The information sought by him vide his RTI application was:

"1. Names of all telemarketers and header/s assigned to them for promotional message in XY-NZZZZZ format, where N is the serial number (1-7) of partially blocked category, indicating the nature of product/ services being promoted. ZZZZZ indicates five digits allocated to particular telemarketer by an access provider;

2. Names of all telemarketers and header/s assigned to them for transactional message XY-ZZZZZZ where X stands for the code allotted to the access provider, Y stands for the service area, ZZZZZZ indicates six alphabets for company or organization sending transactional SMS"

A true Copy of the news article dated 21.04.2020 published by Mr. Yogesh Sapkale on www.moneylife.com has been annexed herewith and marked as **"ANNEXURE P- 53"**

xx. The Petitioner No. 2 again wrote e-mails dated 01.05.2020 to the Respondent Nos. 3, 4, 5, 6 & 8Telcos reiterating that the Respondent Telcos had a statutory obligation under the TCCCPR 2018 to curb unsolicited commercial communication over its network. The Petitioner is yet to receive any response to the same.

True Copies of the E-mails dated 01.05.2020 sent by the Petitioner to the Respondents Nos. 3, 4, 5, 6& 8 are annexed collectively as **ANNEXURE P- 54 (colly).**

yy. On 06.05.2020, a virtual open house discussion was conducted by the Respondent No. 2 Authority wherein the problem of increasing unsolicited commercial communication was discussed with the various Telco. In this regard, Rajan Mathews, Director General, Cellular Operators Association of India (COAI) stressed on the inadequacy of the current regime of financial disincentives on unregistered telemarketer and stated that there is a need for stronger financial disincentives

for UTMs responsible for sending unsolicited commercial communication.

A true copy of the an article by the Economic Times, dated 06.05.2020 on Respondent No. 2's virtual open house discussion is annexed herewith and marked as **"ANNEXURE P - 55 ".**

zz. On 23.05.2020, the Times of India's Ahmadabad Mirror reported that three different complaints totalling Rs. 12.4 lakhs have been registered over a span of three days in Ahmedabad alone, where the son of a former Supreme Court Judge, an orthopaedic surgeon, and an senior citizen, were defrauded using a fraudulent link that sought an update on their Patym Wallet KYC norms.A true copy of the News Article titled *'3 People click fake link, lose Rs. 12.40L'* published on 23.05.2020 by the Ahmadabad Mirror, is annexed as "**ANNEXURE P- 56"**

A true copy of the News Article titled *'3 People click fake link, lose Rs. 12.40L'* published on 23.05.2020 by the Ahmadabad Mirror, is annexed as **ANNEXURE P- 56 .**

aaa. Despite the Petitioner's constant efforts, Telcos'cooperation with the Petitioner has been exceedingly ad-hoc and lacking in systemic prevention as required by the TCCCPR.Whenever a customer of the Petitioner No. 2 reports a fraudulent message header or phone number used for phishing attempts, the Petitioner No. 2 consolidates these complaints and sends them to the Respondent Telcoswith a request to block these message headers and phone numbers. While some of the Respondent Telcos have cooperated with the Petitioners,such

action is only taken when a request to this effect is made by the Petitioner No. 2. Even so, as of May 2020, out of the 5407 report fraudulent phone numbers, only 550 have been confirmed by the Respondent Telcos as having been blocked.

15. It is submitted that the foregoing factual narrative amply demonstrates that despite the existence of a relatively robust regulatory regime and the Petitioners' own efforts, there has been no effective curb on the menace of unsolicited fraudulent commercial communication. This is a direct result of an abject failure on the part of both, the Government Authorities and the Respondent Telcos to implement the TCCCPR and related laws.

16. Therefore the Petitionersare left with no other remedy but to approach this Hon'ble Court on the following grounds, taken without prejudice to each other. The Petitioners crave the leave of this Hon'ble Court to amend and/or add to the same during the course of the proceedings:

GROUNDS

A. Because thecontinued proliferation of fraudulent UCC is a direct result of the failure of the Respondent No.2 Authority and Respondents Nos. 3-9Telcos to effectively implement and comply with their obligationsunderthe TCCCPR, 2018 regime.

B. Because this failure to implement the TCCCPR is further compounded by the failure of the Respondent No.1 Department to effectively implement the DOT Circular on Sim Verification, 2012.

Respondents' amenability to the Writ Jurisdiction of this Hon'ble Court

C. Because Respondents No. 1 and 2 are governmental authorities. Respondent No. 2 is the regulatory body charged with the oversight of implementation of the TCCCPR 2018 while Respondent No. 1 issued and is responsible for the implementation of DOT Circular on Sim Verification, 2012.

D. Because all the Respondents can be held liable for such abdication of their obligations by this Hon'ble Court in exercise of its writ jurisdiction under Art. 226 of the Constitution.

E. Because it has consistently been held by the Hon'ble Supreme Court that the actions of even private companies would be amenable to judicial review under Art. 226 in respect of the discharge of public duties/functions. The Hon'ble Court in *Binny v. V. Sadasivan*(2005) 6 SCC 657 has held that a writ of mandamus can be enforced against a private body if (1) it is discharging a public function; (2) the action of the private body sought to be corrected or enforced is in discharge of the public function; and (3) the public duty is not of a discretionary character. The source of the duty may be statutory or otherwise. 'Public function' was defined by the Hon'ble Court as follows:

> *"11. …A body is performing a 'public function' when it seeks to achieve some collective benefit for the public or a section of the public and is accepted by the public or that section of the public as having authority to do so*
> *…*
> *29. However, the scope of mandamus is limited to enforcement of public duty**. The scope of mandamus is determined by the nature of the duty to be enforced, rather than the identity of the authority against whom it***

> ***is sought. If the private body is discharging a public function and the denial of any right is in connection with the public duty imposed on such body, the public law remedy can be enforced.*** *The duty cast on the public body may be either statutory or otherwise and the source of power is immaterial, but, nonetheless, there must be the public law element in such action…"*
>
> (Emphasis Supplied)

F. Because under Section 4 of the Indian Telegraph Act, 1885, it is the Government that has the exclusive privilege to establish maintain and operate telegraphs (telecom services are essentially telegraphs as defined in Section 3(1AA) of the said Act). However, it also has the power to grant licenses to private bodies to establish, maintain such Telegraphs, and it is under the proviso to Section 4 that the Telcos have been granted their UALs by the Respondent No. 1 Department.

G. Because, the Hon'ble Supreme Court, in ***Secretary, Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal***(1995) 2 SCC 161, inthe context of broadcasting services has described airwaves/frequencies as public property thus:

> *"78. There is no doubt that* ***since the airwaves/frequencies are a public property*** *and are also limited****, they have to be used in the best interest of the society*** *and this can be done either* ***by a central authority by establishing its own broadcasting network or regulating the grant of licences to other agencies, including the private agencies****."*
>
> (Emphasis supplied)

H. Because the said reasoning has been used by the Hon'ble Supreme Court in the 2G Spectrum case, ***Centre for Public Interest Litigation v. Union of India &Ors.,*** (2012) 3 SCC 1 to hold that when telecom licenses are granted to telecom companies, the State is handing over the use of natural

resources which it holds in public trust, and thus must be guided by the doctrine of equality when it transfers such resources to the private domain.

I. Because while the 2G case pertained to the illegalities in the grant of UALs to Telcos, it also established that the Telcos, in getting UALs allotted to them,have been assigned the exclusive privilege/sovereign function of the State to maintain establish and operate telegraphs,

J. Because in ***Ramakrishna Mission &Anr. V. Kago Kunya &Ors.,*** (2019 SCCOnline SC 501), the Hon'ble Supreme Court reviewed the line of decisions on when a writ petition can be maintained against a private entityto hold:

> "*37. Before an organisation can be held to discharge a public function,* ***the function must be of a character that is closely related to functions which are performed the State in its sovereign capacity****."*
>
> (Emphasis Supplied)

K. Because, as stated above, Telcos, in providing telecom services, are performing a function closely related to the State's sovereign functions.Therefore, Telecommunication service providers, i.e. the Respondents Nos. 3 -9Telcos, discharge a public function.This has been recognized by the Hon'ble Supreme Court in ***Delhi Science Forum v Union of India***(1996) 2 SCC 405:

> *"…****telecommunications has been internationally recognized as a public utility of strategic importance***
>
> *Central Government is expected to put such conditions while granting licences, which shall safeguard the public interest and the interest of the nation. Such conditions should be commensurate with the obligations that flow while parting with the privilege which has been exclusively vested in the Central Government by the Act"*

(emphasis Supplied)

The Ld. TDSAT has followed this reasoning in *Reliance Infocomm Limited v. Union of India,* (2005, 3 JB) to hold that:

> *"40. … Nature of duty in telecommunication is such that any licensee under Section 4 could be said to have undertaken to perform public duty."*

L. Because, it is a settled position of law that (as clarified in ***Binny***) and ***KK Saksena V. International Commission on Irrigation and Drainage*** (2015) 4 SCC 670, that even if an entity can be said to be performing a public function, a writ would not lie against the said entity to enforce purely private law (like, for instance, contractual service related) rights.Thus, in ***Jatya Pal Singh v. Union of India*****,** (2013) 6 SCC 452, where a writ Petition was filed against VSNLby its former employees who were allegedly illegally terminated by VSNL, the Hon'ble Supreme Court found the same to not be maintainable. It is submitted that this was because the duty sought to be enforced in ***Jatya Pal Singh***, was a private contract of service, i.e. a private law remedy.

M. Becausehowever, the public duties of the Telcos sought to be enforced by the present Petition are their statutory duties under the TCCCPR regime to take action against the senders of fraudulent & unsolicited commercial communication, as well as safeguarding the fundamental right to Privacy and data integrity of their users under Article 21. Such inaction has resulted in financial losses to the customers of the Petitioners and its associate companies/ related parties/ group

companies, along with reputational and other losses to the Petitioners itself.

N. Because the obligations of the Telcos under the TCCCPR regime are statutory in nature, since the TCCCPR, having been issued under S. 36 read with Section 11 of the TRAI Act, is legislative in nature. The Hon'ble Supreme Court in ***Bharat Sanchar Nigam Limited v. Telecom Regulatory Authority of India***(2014) 3 SCC 222has recognized the legislative nature of such Regulations issued by the Respondent No.2 Authority.

O. Because therefore, the Respondents 3 to 9 Telcos are amendable to this Hon'ble Court's writ jurisdiction for the enforcement of their public law duties sought herein.

Violations of the TCCCPR Regime by the Respondents

P. BECAUSE the TCCCPR 2018 was enacted to balance the consumers' fundamental rights to privacy and data integrity on the one hand with legitimate business interests on the other. The right to privacy was recognized as a constitutionally protected right under Article 21 of the Constitution by a nine-judge bench of the Hon'ble Supreme Court of India in *Justice K.S. PuttaswamyandOrs. vs. Union of India (UOI) and Ors.* (2017) 10 SCC 1, wherein it was held:

> *"177. …Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual. This is evident from the emphasis in the European data protection regime on the centrality of consent.* ***Related to the issue of consent is the requirement of transparency which requires a disclosure by the data recipient of information pertaining to data transfer and use****"*
>
> (Emphasis Supplied)

It isstated that inherent in the above formulation of consent is that consent induced by misrepresentation and fraud would be no consent at all.

Q. Because therefore, the TCCCPR places on the Telcos a **primary duty to prevent**any 'unsolicited' commercial communication being sent over its networks. To this end, the TCCCPR seeks to prohibit and penalize the **senders** of "unsolicited" commercial communication, as well as the **access providers** over whose network such unsolicited &fraudulent commercial communication is being sent. The terms"commercial communication", "unsolicited commercial communication", "consent" and "inferred consent" as defined by the TCCCPR 2018, are reproduced below:

> *"2 (i) "commercial communication" means any voice call or message using telecommunication services, where the primary purpose is to inform about or advertise or solicit business for-*
>
> *(A) goods or services;or*
>
> *(B) a supplier or prospective supplier of offered goods or services; or*
>
> *(C) a business or investment opportunity; or*
>
> *(D) a provider or prospective provider of such an opportunity.*
>
> *Explanation – For the purposes of this regulation it is immaterial whether the goods, service, land or opportunity referred to in the content of the communication exist(s), is/ are lawful, or otherwise. Further, the purpose or intent of the communication may be inferred from:-*
>
> *(A) The content of the communication in the message or voice call;*
>
> *(B) The manner in which the content of message or voice call is presented;*
>
> *(C) The content in the communication during call back to phone numbers presented or referred to in*

the content of message or voice call; or the content presented at the web links included in such communication;

…

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

(i) Any transactional message or transactional voice call;
(ii) Any service message or service voice call;
(iii) Any message or voice calls transmitted on the directions of the Central Government or the State Government or bodies established under the Constitution, when such communication is in public interest;
(iv) Any message or voice calls transmitted by or on the direction of the Authority or by any agency expressly authorized for the purpose by the Authority

…

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

…

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

R. Because all fraudulent communication seeks to masquerade as legitimate commercial communicationby attempting to lure customers through messages and phone calls about investment opportunities, cash prizes, bonuses, completion of KYC formalities, loan opportunities and other seemingly lucrative services and opportunities. Having so lured the customers, the sender then engages in the activity of

'phishing', which has been defined by this Hon'ble Court in *NAASCOM v. Ajay Sood*, 119 (2005) DLT 596, as:

> *"10. ...Phishing is a form of internet fraud. In a case of phishing, a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords, etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party. Typically, phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details"*

S. Because however, all fraudulent commercial communication would come within the meaning of UCC as definedin Reg. 2(bw) of the TCCCPRas it is safe to assume that such fraudulent communication goes against the requirements of both inferred consent and the registered preferences of the recipient in terms of section 2(bw) of the TCCCPR 2018. It can be "inferred" that a recipient of fraudulent message would not have given his consent to the such fraudulent UCC, which in turn makes it obligatory on the part of the Respondent TSPs/ Telcos to ensure that senders of such fraudulent commercial communication are penalized and all such communication is stopped.

T. Because fraudulent & unsolicited commercial communication does not meet the parameters of consent laid down by the TCCCPR 2018 and is therefore in violation of the fundamental right to privacy of the recipients of such fraudulent communication.

U. BECAUSE, in order to protect consumers from UCC, and by extension fraudulent commercial communication, the

TCCCPR, 2018 establishes **primary obligations on the Telcos (referred to as Access Providers) to prevent and penalize UCC**; and **secondary obligations on the Respondent No.2 Authority to prevent and penalize the Telco's violations of the TCCCPR regime**.

V. Because Reg. 3 of the TCCCPR imposes an obligationon an Access Provider to ensure that no UCC takes place over its network, and states:

> *"3. Every Access Provider shall ensure that any commercial communication using its network only takes place using registered header(s) assigned to the sender(s) for the purpose of commercial communication; and*
>
> *(1) NoSubscriber, who is not registeredwithanyaccess provider for the purpose of sending commercial communications under these regulations, shall make unsolicited commercial communication; and*
>
> *(a) in case,any Subscriber issending Commercial Communication, telecom resources of the sendermaybeput underusage cap; and*
>
> *(b) if the Subscriber continues to sendCommercialCommunicationdespitenoticegive n to him under these regulations,all telecom resources ofthe sender may also be disconnected."*

W. Because the aforesaid envisages twotypes of obligations on the Access provider: (i) **a duty to prevent**which kicks in *prior* to *any* commercial communication taking placeover its networks, and (ii) a **duty to penalize/punish** or take remedial action once UCC or fraudulent commercial communication is found to have taken place over an Access Providers telecom network.

Violations by Telcosof the Duty to Prevent under the TCCCPR Regime

X. Because the Access Providers' duty to preventis operationalised by the TCCCPR mandating the use of Distributed Ledger Technologies for(i) the mandatory registration of consumer preferences for receipt of commercial communication and (ii)the mandatory registration of all sender(s) (referred to as registered telemarketers or RTMs) that intend to send commercial communication over an Access Provider's telecom network. The provisions of the TCCCPR pertaining to this duty to prevent are reproduced below:

> *"5. Every Access Provider shall develop an ecosystem with the following functions to regulate the delivery of the commercial communication as provided for in these regulations:-*
>
> *(1)* ***to provide facility to its subscribers for registering preference(s) for Commercial Communication*** *and maintain complete and accurate records of preference(s);*
>
> *(2) to register entities for participating in the ecosystem and prescribe their roles and responsibilities for efficient and effective control of commercial communication;*
>
> *…*
>
> *(5)* ***to register sender(s), carry out verifications of their identifies*** *and prescribe processes for sending commercial communication.*
>
> *(6) to prescribe process and specific functions of particular entity* ***to carry out pre-delivery checks before sending commercial communicatio****n and ensuring regulatory compliance"*
>
> *…*
>
> *"7. Every Access Provider shall ensure that preferences recorded or modified by the Subscriber* ***are given effect to in near real time and in such a manner that no delivery of commercial communication is made*** *or blocked in contravention to*

the Subscribers' preference after twenty-four hours or such time as the Authority may prescribe."

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

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

Y. BECAUSE the aforesaid provisions of the TCCCPR clearlyexplain the Access Providers' duty to prevent. The use of DLT ensures traceability by mandating registration at every level, namely:-

a. Registration of entities such as the Petitioner No. 2
b. **Registration of the official headers used by such entities**,
c. **Registration of the content template of the message**,
d. Registration of consent by customer and/ or their preference to receive messages/ phone calls from a particular header/ particular entity

This ensures that entities send communication to only customers who have shared specific (not generic as per earlier guidelines under the TCCCPR 2010) consent on SMS template, header and entity. It also makes the sender of unsolicited and fraudulent commercial communication traceable, such that they can be blocked centrally across Telcos. The DLT also introduces transparency since each Telco has access to all entities, headers registered and

their respective templates registered with every other Telco. It is submitted that the adoption of this technology has the potential to make the sending of Bulk SMSes completely fraud-proof and transparent. It will reduce SMSes falling under the category of UCC (Unsolicited Communications) to negligible levels and provide a safe and private space to mobile subscribers. However, the Respondent Telcos have failed to fully operationalize theDLT.

Z. BECAUSE such registration is mandated to be accompanied with **verification**of the identities before such senders can be registeredin accordance with the Code(s) of Practice – Entitiesto be established by the Access Provider under Reg. 8(1)in accordance with Schedule I.Clause 4 of Schedule I describes the 'Header Registration Function' (hereinafter "HRF") and the 'Content Template Registration Function' (hereinafter "CTRF") of each TSP/ Telcosas:

> *"4. Every Access Provider shall carry out following functions: -*
>
> *(1) Header Registration Function (HRF)*
>
> *a)* ***assign header or Header root for SMS via Header Registration Functionality, on its own or through its agents****, as per allocation and assignment principles and policies, to facilitate content provider or principal entity to get new headers;*
>
> *b)* ***carry out pre-verifications of documents and credentials submitted by an individual, business entity or legal entity requesting for assigning of the header****;*
>
> *c)* ***bind with a mobile device and mobile number(s), in a secure and safe manner, which shall be used subsequently on regular intervals for logins to the sessions by the header assignee****;*

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

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

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

(2)…

(3) Content Template Registration Function (CTRF):-

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

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

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

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

(e) to generate one-way hash for fixed portion of content of template and ways to extract fixed

portion and variable portion(s) from actual message for carrying out pre and post checks of actual content of actual message offered for delivery or already delivered;

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

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

(Emphasis Supplied)

AA. Because therefore, if properly implemented, the TCCCPR regime would ensure that:

a. only registered entities (RTMs) are able to send commercial communication;

b. that such RTMs are assigned headers that are unique and not deceptively similar to those of other entities and don't mislead the consumer as to the identity of the sender;

c. that such RTMs are assigned unique template identities; and

d. that the identity of such RTMs is thoroughly verified before registration by the Access Provider.

It is therefore submitted, that not only must no look-alike header be issued by the Respondent Telcos to fraudsters, but there must also be checks by the Respondent Telcos to make sure that the content of the message is not misleading. It is submitted that if the aforesaid were to be followed by the respondent Telcos there would be no fraudulent UCC being sent to consumers

BB. Because however, the manner in which fraudulent UCC from RTMs takes place demonstrates that the Respondent Telcoshave blatantly failed to comply with their duty to prevent obligations under the TCCCPR regime. In particular, by failing to thoroughly verify the identities of sender(s), the Respondent Telcos have assigned look-alike header(s), header root(s) and content templatescontaining words like “Paytm”, “PTM” ,“Pytm” etc, which aredeceptively similar to the Petitioners’ and its associate companies/ group companies’ official header(s)/Root(s)/contempt template(s), to unscrupulous fraudsters. The fraudsters then use these headers/ content templates to communicate with and dupe the customers of the Petitioners and its associate companies/ related parties/ group companies in the manner explained in paras 13(i) and (k) above. The Telcos, having failed to prevent the registration of misleading headers have also failed to ensure that the content of the UCC is not misleading. Thus, it is submitted that the Telcosare in gross violation of their Duty to Prevent fraudulent UCC as envisaged in the TCCCPR Regime, in particular, Regs. 3,5(3), 12(2), 12(3), 13(1) and Clause 4 of Schedule I to the TCCCPR.

CC. Because further, Reg. 20 read with Reg. 8 mandates that every Access Provider formulate a Code of Practice in accordance with the Schedules and complies with the provisions of the same. In the present matter, only Respondent Nos. 3, 5, 6 & 7 have formulated any COP at all and these are available in the public domain. Thus Respondents Nos. 4 and 8 Telcos are also in violation of their obligations under Reg. 8.

DD. Because moreover, even the CoPs formulated by the Respondents 3, 5, 6 & 7, are not in compliance with the TCCCPR, Schedules read with Regulation 8. Further, the actual process adopted by the Respondent Telcos qua verification of entities prior to registration, appears to be in contravention of their own published CoPs. Thus, it is apparent that even the published CoPs are merely paying lip service to the regulatory mandate, and are not implemented on the ground.

Violations by Telcos of the Duty to Penalize/ Punish under the TCCCPR Regime

EE. Because the TCCCPR also provides for the Telcos to take punitive action against sender(s) of unsolicited and fraudulent commercial communication, with the Telcos' overcharging obligation being Reg. 3. Reg.3 casts on the Telcosanobligation upon the Respondent TSPs/ Telcos to ensure that commercial communications sent over its network take place only through registered message headers and phone numbers. It further empowers the Access Providers to take punitive action(i.e. putting of usage caps, or, in case of repeated violations, the disconnection of all telecom resources) against subscribers who send unsolicited commercial communication without requisite registration of headers/ phone numbers, in violation of the said provision of the TCCCPR 2018.

FF. Because apart from reg.3, the other Duty to Penalize/Punish Obligations of the Telcos/Access Providers are reproduced below:

> *"5. Every Access Provider shall develop an ecosystem with the following functions to regulate the delivery of the commercial communication as provided for in these regulations:-*
> *...*
> *(8) to examine and investigate complaints, take actions against defaulters and* ***take remedial measures*** *to ensure compliance with these provisions.*
> *(9)* ***to detect, identify and act against sender(s) of Commercial Communication who are not registered with them****."*
>
> ***"****12.* ***Access Providers shall deploy, maintain and operate a system****, by themselves or through delegation****, to ensure that requisite functions are performed in a non-repudiable and immutable manner:-***
>
> ***...***
>
> *(7)* ***To detect non-compliance and take immediate action*** *to effectively ensure compliance with regulations;"*
>
> *"23.* ***Every Access Provider shall establish Consumer Complaint Registration Facility (CCRF****) and shall make necessary arrangements to facilitate its customers on 24 hours X 7 days basis throughout the year:-*
>
> *(1****) to provide ways and means:-***
>
> ***(a) to make complaint(s), by its customer who has registered his preference(s),*** *against sender(s) of unsolicited commercial communication in violation of the registered preferences or digitally registered consents;*
>
> *(b)* ***to submit report(s,) against sender(s) of commercial communication in violation of provisions of these regulation(s) by any customer****. …"*
>
> (emphasis Supplied)

FF. Because therefore, the Telcos are mandated to register complaints and/or reports by *any* customer

(irrespective of whether such customer has registered preferences or not) of violations of the TCCCPR. The Telcos are also mandated to *suomotu* (as is demonstrated by a reading of regs. 5(9) and 12(7) action against senders violating the TCCCPR. Thus, the said duty to penalise as encapsulated in the TCCCPR is very wide.

GG. Because under Reg. 23 the Telcos are also obligated to have systems in place to register "reports" from not just recipients of UCC but, under Reg. 23(1)(b) **from any person**, regarding the violations of the TCCCPR by senders of UCC. The Petitioners are customer-senders of the Telcos, within the meaning of Reg. 2(bf) read with Reg. 2(u) and 2(bn). The aforesaid Regulations read as follows:

*"2(u) '**Customer' means subscriber***
*2(bf) '**Sender**' in relation to a commercial communication, means*

i. ***The person of entity who owns the telephone number of the header(s) that were used**;*
ii. *A person or entity that publicly asserts or uses a Calling Line Identity (CLI) or the phone number(s) referred to in the communication except where such assertion is fraudulent;*
iii. ***The person who sent the message or made a voice call, caused the message to be sent or the voice call to be made or authorized the sending of the message or making of the voice call**;*
iv. *The person of legal entity dealing with goods, or services, or land or property, or a business or investment opportunity that is offered or prompted; except where such entity maintains a distinct legal identity for the division or line of business dealing with offered goods, services or opportunity, in which case such division or line of business.*

*2(bn) '**Subscriber' means a person or legal entity who subscribes to a telecom service provided by an Access Provider**."*

(Emphasis Supplied)

HH. Because therefore, the Petitioners, being subscribers of the telecom services of the Respondent Telcos for the purpose of sending commercial communication, is also a customer of the Respondent Telcos and it is incumbent upon the Respondent Telcos under Reg. 23(1)(b) to have mechanisms in place to register reports from the Petitioners of violations of the TCCCPR by fraudsters misrepresenting themselves to be the Petitioners or its associate companies/ related parties/ group companies. However, no such mechanism is in place and the Petitioner No. 2 has been regularly e-mailing/writing letters to the Respondent Telcoswith its reports of such violations of the TCCCPR. Thus, the respondent Telcos are in violation of their obligations under Reg. 23(1)(b).

II. Because the mechanism for Complaint Redressal is provided in Reg. 25, which makes a distinction between the remedial action to be taken by the Telcos against Registered Telemarketers (RTMs), and Unregistered Telemarketers (UTMs). While the Petitioners have also challenged the constitutionality of the TCCCPR penalty regime against UTMs (which will be adverted to in the subsequent Grounds), it is submitted that the Telcoshave woefully failed to meet their obligations of taking remedial action against both, RTMs and UTMs.

JJ. Because Reg. 25 distinguishes between the roles of the Originating Access Provider (OAP) and Terminating Access Provider (TAP), with the OAP being the Telco from whose network the UCC is sent, and the TAP being the Telcoto

whose network the recipient of the UCC subscribes.The customer must make his complaint to the TAP, who in turn will forward the complaint to the OAP. The OAP is then responsible for all fraudulent communication taking place over its network. The Complaint Mechanism under Reg. 25, in relevant part, is reproduced below:

> *25. Complaint Mechanism:*
>
> *...*
>
> (4) ***The OAP, in case the complaint is related to Registered Telemarketer (RTM), shall examine, within one business day from the date of receipt of complaint, whether all regulatory pre-checks were carried out in the reported case before delivering Unsolicited Commercial Communications****; and*
>
> (a) *In case, all regulatory pre-checks were carried out and delivery of commercial communication to the recipient was in confirmation to the provisions in the regulations and Code(s) of Practice, OAP shall communicate to TAP to inform complainant about the closure of complaint as provided for in the Code(s) of Practice;*
>
> (b) ***in case of non-compliance with the regulations, the OAP shall, within two business days from the date of receipt of complaint, take actions against the defaulting entity and communicate to TAP*** *to inform the complainant about the action taken against his complaint as provided for in Code(s) of Practice;*
>
> (c) ***the OAP shall take appropriate remedial action, as provided for in the Code of Practice(s****), to control Unsolicited Commercial Communications so as to ensure compliance with these regulations;*
>
> (5) *The OAP,* ***in case, the complaint is related to an Unregistered Telemarketer (UTM****),*
>
> (a) *shall examine communication detail records (CDRs), within one business day from the date of receipt of complaint, to check the occurrence of complained communication between the complainant and the reported telephone number or header from which unsolicited commercial communication was received.*
>
> (b) *In case of no occurrence of complained communications under sub-regulation (5)(a), OAP*

shall communicate to the TAP to inform the complainant about the closure of complaint in a manner prescribed in the Code(s) of Practice;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

KK. Because the Respondent Telcoshave violated their obligations to take actions against both,non-compliant/fraudulent RTMs and UTMs.As has been demonstrated by the factual averments above, the Petitioner No. 2 has consistently been reporting fraudulent headers/ short codes and the like to the Respondent Telcos, but only a fraction of such reported fraudulent headers havebeen confirmed by the Respondent Telcos as having been blocked, which is in stark violation of the TCCCPR. In fact, the Petitioner No. 2 has also received communications from the Telcos, such as the e-mail dated 31.01.2020 from respondent No.7, informing it that the said respondent would not block any access to telecom services of a fraudulent sender unlessso directed by the government or law enforcement authorities. Further, when the Petitioner sought information from the Telcoson the List of Headers which had been found to be responsible for fraudulent/fake messages, so that it could identify the same and take action at its own end (such as the e-mail dated 17.03.2020 sent to Respondent No.6 Telco), it wasinformed yet again, that the Telco was not an investigating agency and that it should file complaints with relevant law enforcement agencies (E-mail dated 27.03.2020 from Respondent No.6 Telco to the Petitioner No. 2). It is submitted that this is not only in violation of the Telcos' duty to penalise and punish under the TCCCPR but also militates against the very ethos of the TCCCPR regime, which is a self -contained code with all capacity to identify and take action against violations by fraudulent senders.

LL. Because with respect to UTMs, it is submitted that as per Regulation 25(6)(c) of the TCCCPR 2018, upon the third and subsequent instances of violation by the sender of unsolicited commercial communication, there shall be complete disconnection of all telecom resources of the sender, and all other access providers shall also be asked to put such sender on a blacklist so as to not allot any new telecom resources to such sender. Thus, regulations 3 read with 25(6) empower the access providers to be able to take punitive action against senders of unsolicited, and fraudulent, commercial communication.

MM. Because in this regard, the Petitioner No. 2 has repeatedly sent the Respondent Telcosall relevant details of the mobile numbers of reported reported UTMs along with “first instance”, “second instance” and “third instance” violations by Senders, as per complaints received, and sought the immediate blocking of such numbers (E-mails from the Petitioner No. 2 dated 23.01.2020 and 02.03.2020, and Legal Notices dated 28.02.2020). However, adequate action has not been taken by the Respondent Telcosagainst such fraudulent UTMs.

Violations by the Respondent Telcos of their public law duty to ensure that no fraud takes place over their Telecom Networks

NN. Because, apart from the above, it is submitted that the Respondent Telcos, having been licensed the privilege of establishing, maintaining and operating telecom networks under the Telegraph Act, carry out public functions, and are therefore also entrusted with non-statutory public duties. In

particular, such Telcos are entrusted to ensure that their networks are not used to carry out fraudulent activities, which the Respondent Telcos have clearly failed to do.

Violations by Respondent No.2 Authority of its Obligations under the TCCCPR

OO. Because, as stated above, the TCCCPR imposes two layers of obligations, i.e. primary obligations on the Telcos to prevent and punishviolations by senders; and secondary obligations on the Respondent No.2 Authority to prevent and penalize the Telco's violations of the TCCCPR regime. The obligations of the Respondent No.2 Authority are reproduced below:-

> "*21.* ***In case of non-compliance to the provisions of Code(s) of Practice, Access Provider shall be liable to pay, by way of financial disincentive****, following amount:*
>
> 1. *not exceeding Rupees five thousand per day for the period of exceeding the timeline if the period of delay is less than or equal to thirty days;*
> 2. *not exceeding Rupees twenty thousand per day for the additional period of delay which is more than thirty days;*
>
> *The amount payable by way of financial disincentive under these regulations shall be remitted to such head of account as may be specified by the Authority.*
>
> *The total amount payable as financial disincentives under sub-regulations (1) and (2)shall not exceed rupees ten lakhs.*
>
> *The Authority reserves the right not to impose financial disincentive or to impose a lower amount of financial disincentive or no incentive where it finds merit in the reasons furnished by the access provider.*
>
> *Provided that no order for payment of any amount by way of financial disincentive shall be made by the Authority, unless the concerned Access Provider has been given a reasonable opportunity to represent."*

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

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

	Value of "Counts of UCC for RTMs for one calendar month"	*Amount of financial disincentives in Rupees*
(a)	*More than zero but not exceeding hundred*	*Rupees one thousand per count*
(b)	*More than hundred but not exceeding one thousand*	*Maximum financial disincentives at (a) plus Rupees five thousand per count exceeding hundred*
(c)	*More than one thousand*	*Maximum financial disincentives at (b) plus Rupees ten thousand per count exceeding one thousand*

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

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

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

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

(1) Power of Authority to order inquiry: -

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

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

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

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

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

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

Provided that no order for payment of any amount by way of financial disincentive shall be made by the Authority, unless the concerned Access Provider had been given a reasonable opportunity of representing against the findings of the inquiry committee. The amount payable by way of financial disincentive under these regulations shall be remitted to such head of account as may be specified by the Authority. The total amount payable as financial disincentives under sub-regulations (2)(a) and (2)(b) shall not exceed rupees ten lakhs in a week.

(3) The Authority may impose no financial disincentive or a lower amount of financial disincentive than the amount payable as per the

provisions in sub-regulations (2)(a) and 2(b) where it finds merit in the reasons furnished by the access provider"

(Emphasis Supplied)

PP. Because the Respondent No.2 has failed to comply with its oversight obligations envisaged in the aforesaid provisions. In particular, it is submitted that it has failed to take action against the Respondent Telcos under Reg.21 for the Telcos' non-compliance with the CoPs as mandated by Reg. 20. In essence, Regulations 8 and 20 of the TCCCPR 2018, read with Regulation 21 provide for a mechanism for the Access Providers to be penalized for non-compliance of the Header Registration Function to detect and prevent deceptively similar headers being issued to any of the users as well as the Content Template Registration Function. It is submitted that the sheer number of cases of fraudsters sending messages through the networks of the Respondent TSPs makes it abundantly clear that the above-mentioned provision of TCCCPR, 2018 is not being complied with. The Respondent No.2's failure to take action against such Telcos is itself an abdication of its obligations under Reg. 21.

QQ. BECAUSE Regulation 27 of the TCCCPR, 2018 lays down the financial disincentives that can be levied on the Respondent No. 3 to 8 Telcos if they fail to curb unsolicited commercial communications sent through their networks. Such financial disincentive is to be levied on the Respondent No. 3 to 8 Telcos by the Respondent No. 2 Authority. Despite the Respondent Telcos' failure to curb such fraudulent UCC, the

Respondent No.2 Authority appears to have failed to take any action against them, in violation its own obligations under Reg. 27.

RR. Because the Respondent No.2 Authority has failed to initiate any inquiry/action against the Respondent Telcos under Reg. 28, for the violation by the Telcos of their primary prevention (i.e. **robust verification before registration of entities**) duties elaborated above.

SS. Because despite the Respondent No. 2 authority having the power under Regulations 27 and 28, to carry out an inquiry and penalize the Respondent Telcos for failing to implement the provisions of the TCCCPR 2018, the same is not being done. Despite having such over-arching powers in its capacity of the Regulatory body governing the Telecom operators or Telecom Sector companies, the Respondent No. 2 has failed to play the guiding and supervisory role for which it was constituted under the provisions of the TRAI Act, 1997.

TT. Because the Respondent No.2 Authority is further empowered under Sections 12 and 13 of the TRAI Act conduct investigations into the affairs of the Respondent Nos. 3 to 9 and seek information from them, so as to ensure that they take necessary steps to prevent fraudsters from duping the customers of the Petitioners and its associate companies/ related parties/ group companies, and to issue orders to this effect under section 13 of the TRAI Act, 1997 to ensure that standards of quality of services provided by the Service Providers in the Telecom Sector are being maintained. Yet it has failed to take any such action, despite the requests of the

Petitioners, thereby necessitating the Petitioners having to approach this Hon'ble Court for relief.

Unconstitutionality of Reg. 25(5) and 25(6) in respect of the Penalties imposed on UTMs

UU. BECAUSE Reg. 25(5) and 25(6) of the TCCCPR, insofar as they impose a graded penalty on UTMs, and that too on the basis of whether the UTM has sent bulk UCC or not, is in violation of the fundamental right to privacy, *ultra vires* the TCCCPR's parent statute, i.e. the TRAI Act and also inconsistent with the other provisions of the UTM.

VV. Because privacy has been recognized by the Hon'ble Supreme Court as part of a person's fundamental right to life and liberty under Art. 21 of the Constitution. Thus **any** commercial communication would impinge on the privacy of individuals in general, as the senders of such communication would be provided access to the consumers' contact details by Telcos. Unsolicited Commercial Communications, as the Respondent No.2 itself notes in the Explanatory Memorandum to the TCCCPR, 2018, seriously violate customers' fundamental right to privacy

WW. Because the TCCCPR has therefore sought toachieve a balance between customers' rights to privacy and the legitimate commercial interests of businesses, by adopting a two-pronged approach, namely:-

i. The Customer has the right to decide what kinds of commercial communications they wish to receive, by mandating the registration of customer preference; and

ii. **The identification and verification of all commercial communications** carried out over a telecom network by mandating the registration of all entities wishing to send commercial communications as RTMs with Telcos(Reg.3(1)), while prohibiting the sending of any commercial communication by an UTM (Reg.32)

XX. Because the distinction between RTMs (which are, due to registration and verification traceable) and UTMs (which, not being registered in the Telcos UCC ecosystem, may not be so easily traceable) is therefore imperative. It is for this reason that the TCCCPR under Reg. 32 mandates a blanket ban on *any*commercial communication that does not have the actual or inferred consent of its target for a sender who has not registered itself as a telemarketer, i.e. a ban on all unsolicited commercial communications from UTMs. Inpractice however, a large chunk of UCC (and by extension, fraudulent phishing) emanates from UTMs, despite the prohibition on such communication.Thesending of UCC by a UTM therefore violates customers' fundamental rights to privacy and also does not fall within the realm of balancing legitimate business interests. It is also in violation of the stated purpose of the TRAI Act, to protect consumer interests and rights.

YY. Because therefore, it follows that the detection and confirmation of unsolicited commercial communication by even a single UTM, should result in the complete disconnection of all telecom resources of the sender. This is consistent with the interpretation of the true import of Reg. 3(1), read with Reg. 5(9) and reg. 32.

ZZ. Because however, the TCCCPR in Regs. 25(5) and 25(6) provides for action only against certain types of UTMs (i.e. those who send UCC in bulk), and provides for graded penalties (dependant on number of violations by the UTM in question). This, it is submitted, is in violation of customers' fundamental rights to privacy, *ultra vires* the TCCCPR's parent TRAI Act and also inconsistent with the true import of the TCCCPR framework itself.

AAA. Because therefore, Reg. 25(5) and 25(6) insofar as they classify UTMs on the basis of bulk messaging and impose a graded penalty on the basis of the number of violations by the UTM, merit to be struck down as unconstitutional and ultra vires the TRAI Act.

BBB. Because the senders of fraudulent commercial communication have already caused huge losses to the Petitioners by damaging its reputation and continue to cause injury to the customers of the Petitioners and its associate companies/ related parties/ group companies. There has been an irreparable loss to the Petitioners' business reputation, and goodwill due to this fraudulent commercial communication being sent through the respective networks of the Respondent Telcos. Additionally, as a result the losses that the customers of the Petitioners and its associate companies/ related parties/ group companies have suffered, many such customers have filed FIRs against the Petitioners and its officials. There has been a deceleration in the growth of the customer base of the Petitioners.

Failures of the Respondent No.1 Department to take action against the Respondent Telcos' Violations of SIM Verification Obligations

CCC. Because most UTMs use mobile numbers/sim cards that have been issued without proper verification, which makes the senders difficult to trace even for Telcos over whose networks the UCC by the UTM has been sent.

DDD. Because the sale and activation of such SIM cards without proper verification is in violation of the DoT Circular on Sim Card Verification, 2012, and the Respondent No.1 Department has failed in its duty to take action against such violations of the said Circular.

EEE. Because moreover the Respondent Telcos are also obligated under their respective Unified Access License Agreements to ensure adequate verification of each and every subscriber. In this regard, Clause 39 of the UAL Agreement, in relevant part, states

> *"39.17 (i)* ***The Licensee shall ensure adequate verification of each and every customer before enrolling him as a subscriber****; instructions issued by the Licensor in this regard from time to time shall be scrupulously followed. The Licensee shall make it clear to the subscriber that the subscriber will be responsible for proper and bonafide use of the service.*
>
> *39.17 (ii)* ***Format prescribed by the Licensor delineating the details of information required before enrolling a customer as a subscriber shall be followed by the Licensee****. A photo identification of subscribers shall be pre-requisite before providing*

the service. The Licensor may prescribe service-wise detailed instructions for enrolment of subscriber and activation of service from time to time.

39.17(iii) ***The Licensee shall activate the Leased Line, Internet Leased Line and IPLC service only after checking the bonafide of the customer, verifying details as per Customer Acquisition Form (CAF) prescribed from time to time and physical inspection of the site****. Further, in the case of Leased Line, the reasons for taking the link by the customer shall be recorded*

…

39.21 (i) ***Calling Line Identification (CLI) shall be provided. The network should also support Malicious Call identification and Centralized Automatic Message Accounting (CAMA).***

39.21 (ii) Calling Line Identification (CLI) shall never be tampered as the same is also required for security purposes and any violation of this amounts to breach of security.

39.22 (i) ***Utmost vigilance should be exercised in providing bulk connections for a single user as well as for a single location.*** *Provision of 10 or more connections may be taken as bulk connections for this purpose.* ***Special verification of bonafide should be carried out for providing such bulk connections. Information about bulk connections shall be forwarded to respective Telecom Enforcement, Resource & Monitoring Cell and any other officer authorized by Licensor from time to time as well as all Security Agencies on monthly basis****.*

39.22 (ii) The call detail records for outgoing calls made by customers should be analyzed for the subscribers making large number of outgoing calls

day and night and to the various telephone numbers. Normally, no incoming call is observed in such cases. This can be done by running special program for this purpose. ***The service provider should devise appropriate fraud management and prevention programme and fix threshold levels of average per day usage in minutes of the telephone connection; all telephone connections crossing the threshold of usage should be checked for bonafide use. A record of check must be maintained which may be verified by Licensor any time. The list/details of suspected subscribers should be informed to the respective TERM Cell of DoT and any other officer authorized by Licensor from time to time****.*

39.22 (iii) ***Active support must be extended by the service providers to the respective TERM cells of DoT for detection of clandestine / illegal telecommunications facilities.*** *For this purpose, names of the Nodal officers & alternate Nodal Officers in respect of each licensed service area as communicated to the Intelligence Agencies for monitoring of telecommunications should also be forwarded to respective TERM cell of DoT, and any other officer authorized by Licensor from time to time. The TERM Cell of DoT will contact the Nodal Officer / alternate Nodal officer, and till the time such nomination is received or in case of non-availability of such officer, the TERM Cell will contact the Chief Executive Officer of the Licensee, for such support / coordination.*

39.22 (iv) Bulk users premises should be inspected by the service providers at regular intervals for satisfying themselves about bonafide use of such facilities. A record of such inspection should be maintained and preserved for minimum one year, for

inspection / verification by the licensing authority or a designated officer of the authority."

(Emphasis Supplied)

FFF. Because therefore, the Respondent Telcos are mandated to not only curb fraud taking place over their networks but also to report such frauds to the TERM Cell in case of fraudulent bulk users, which are essentially UTMs. However, the Respondents have failed to take any such action, to the best of the knowledge of the Petitioners. The Respondent No.1 Department has also clearly not enforced such obligations.

GGG. BECAUSE the Petitioner No. 2 has approached the Respondent Telcos as well as TRAI, Department of Telecommunications, CERT-In and the Ministry of Home Affairs, several times, but to no avail. The MHA being the agency for enforcing preventive and corrective measures for internal security, CERTIN as the nodal agency for responding to computer security incidents and TRAI being the authority for telecom services, close co-ordination between them will ensure better preparedness and response to phishing activities. A specific and action oriented framework among the aforementioned agencies on dealing with such frauds emanating from the use of telecom services is required. If standard operating procedures such as a protocol for authorities to accept fraud complaints so as to ensure near real time corrective measures is put in place, it would drastically limit fraud over telecom networks.

HHH. Despite repeated attempts of the Petitioners at seeking redressal on behalf of its customers who have been defrauded of large sums of money, the Respondents Telcos have failed to discharge their statutory obligation under the TCCCPR 2018. As a result not only do the grievances of the customers of the Petitioners and its associate companies/ group companies remain unaddressed, but the Petitioners themselves have suffered a loss in reputation and is being held liable by several customers for no fault of their own. It is reiterated that the Petitioners have taken all steps necessary to protect its customers and has complied with the various circulars issued from time to time by the Reserve Bank of India in this regard.

III. Because in public interest it is necessary to enforce regulations to stop online phishing activity to protect the integrity of the online payment systems and to hold the Respondent Telcos accountable for non-compliance of their statutory duty under the TCCCPR 2018 in public interest. However, it is also important that till such time as the mechanisms under the TCCCPR 2018 are completely operationalized, in order to curb existing phishing activity, the reported fraudulent look alike headers deceptively similar to the official headers of the Petitioners and its associate companies/related parties/group companies be blocked, and a stop also be put to the future issuance of such look alike headers. Further, reported phone numbers from which customers of the Petitioners and its associate

companies/ related parties/ group companies have received fraudulent phone calls must also be blocked.

JJJ. BECAUSE on account of the TCCCPR 2018 being relatively recently enacted regulations, in the eventuality that these provisions cannot be implemented for want of technological architecture and solutioning infrastructure, the provisions of the TCCCPR 2010, especially with respect to UTMs must be given effect to the extent of curbing the menace of unsolicited commercial communication over the Respondent Telcos network. The mechanism provided for in the TCCCPR 2010 is as follows:

- Regulation 14 of the TCCCPR 2010 mandated registration by the access providers of all telemarketers who wish to send commercial communication over the network of such access provider. Under Regulation 17, allocation of telecom resources to a telemarketer could only take place after such registration. Regulation 17 provided for a detailed verification process to be carried out by the access provider before allocation of telecom resources. It also required a commercial agreement (with, if desired, provisions for a security deposit by the telemarker) betweensuch registered telemarketer and the access provider.
- Regulation 18 of the TCCCPR, 2010 provided for the blacklisting of the telemarketers either:

a. Upon failure of the telemarketer to pay the deposit amount to the service provider; or

b. Upon the issuance of the sixth notice in a calendar year by any Access Provider on such telemarketer for sending unsolicited commercial communication.

Even under the old regime of TCCCPR, 2010it was incumbent upon the Respondent telecom companies under Regulation 19 to investigate a complaint against UCC sent by a telemarketer to a subscriber who has registered his preference under “Provider Customer Preference Register” and to take action within not more than 6 days from date of receipt of complaint by the telecom companies. If it was found that the call or SMS was an Unsolicited Commercial Communication, the Respondent Telcos were also invested with the power to deduct a certain sum from the security deposit amount as was previously agreed upon between the telemarketer and them, in terms of the commercial agreement entered between them.

KKK. BECAUSE under the old TCCCPR regulations of 2010, the telecom companies were also empowered to take more stringent action against unregistered telemarketers, which is more consistent with the objects of the TRAI Act than the present regime. Under Regulation 19 (11) if the unsolicited commercial communication originated from a subscriber who is not registered with the Authority as a telemarketer, it could issue a notice to such subscriber to forthwith discontinue the sending of such unsolicited commercial communications and at a second instance of violation by a subscriber, the Telcos were empowered to disconnect the telecom resources of such subscriber.

LLL. Because it is evident that due to the non-implementation of the new TCCCPR 2018 and callous approach of the Telecom companies toward the problem of UCC, Respondent No. 2, Authority, had in its direction dated 20.01.2020 directed the Respondents to fulfil their existing mandate under TCCCPR 2018. Pertinently, no action against the Respondents was taken by the authority even after the acknowledged inaction of the Respondent telecom companies for 2 years. Pertinently, no action, whatsoever, was ever taken by the authority against the telecom companieseither under the old regime of 2010 or under the extant one.The Petitioners submits that since the present petition seeks issuance of a writ in the nature of mandamus, the present writ petition is maintainable.The Respondent No. 2authority and Respondent No.1 Departments fall within the ambit of Article 12 of the Constitution of India, while as mentioned above, the Respondent Telcos are performing public functions, and therefore this Hon'ble Court has the jurisdiction under Article 226 of the Constitution to adjudicate upon the present writ petition.

17. The Petitioner submits that it has no alternative, efficacious remedy under the law except to approach this Hon'ble Court by way of the present Writ Petition under Article 226 of the Constitution of India.

18. The balance of convenience and/or inconvenience entirely lies in favour of passing of orders as prayed for herein.

19. The Petitioners have served an advance copy of the present Petition (with annexures) to the Standing Counsels for the Respondents Nos. 1 and 2 via e-mail, and has also served an advance copy of the present Petition (with annexures) to the Respondents Nos. 3 to 9 Telcos on their official e-mail addresses as available on the website of the Ministry of Corporate Affairs, and has also informed them of the same via telephone. True Copies of Proof of service to the Respondents are collectively annexed as **Annexure P - ____ (colly).**

20. This Petition is made bona fide and in the interest of justice and unless orders as prayed for herein are passed, the Petitioner will suffer irreparable loss, prejudice and injury.

PRAYER

In the aforesaid facts and circumstances it is respectfully prayed that this Hon'ble Court may be pleased pass awrit,order or direction in the nature of mandamus, or any other writ, direction or Order to:

a) Declare that Regulations 25(5) and 25(6) of the Telecom Commercial Communications Customer Preferences Regulations, 2018 insofar as they allow the imposition of a graded penalty on identified unregistered telemarketers as unconstitutional and ultra vires the Telecom Regulatory Authority of India Act, 1997;

b) Declare that under Reg. 23(1)(b) of the Telecom Commercial Communications Consumer Preferences Regulations, 2018, the Respondents Nos. 3 to 9 are obligated to put in place mechanisms to register reports of violations from customers like the Petitioners.

c) Direct the Respondent No. 2 Authority to ensure complete and strict implementation of provisions of the Telecom Commercial Communications Customer Preferences Regulations, 2018 and any other related regulations issued from time to time to curb fraudulent unsolicited commercial communication sent over the respective networks of the respondent telecom service providers;

d) Direct the Respondent no. 2 Authority to take action against the Respondents no. 3 to 9 Telcos under Regulations 21, 27 and 28, for violations of their primary obligations of prevention and verification under the Telecom Commercial Communications Consumer Preferences Regulations, 2018;

e) Direct the Respondent No.1 Department to take action to ensure that no sim card is sold without proper verification by effective implementation of the Department of Telecommunications Circular dated 09.08.2012 titled *"Instructions on Verification of New Mobile Subscribers (Pre-paid and Postpaid)"*;

f) Direct the Respondent No.1 Department to ensure effective implementation by the Respondent Telcos of their obligations under their Unified Access License Agreements pertaining to verification and reporting of frauds taking place over their networks;

g) Direct the Respondents Nos. 1 and 2 to establish an Inter-Agency Task Force that includes Computer Emergency Response Team (Ministry of Information and Technology) the Ministry for Home Affairs, Leading Banks and Leading

PPI Wallet issuers to coordinate action limiting fraud over telecom networks;

h) Direct the Respondents Nos. 3 to 9 Telcos to take effective action under the Telecom Commercial Communications Consumer Preference Regulations 2018, to block the phone numbers of UTMs sending unsolicited commercial communication including through phone calls, to the Petitioners' customers.

i) Direct the Respondent No. 3 to 9 Telcos to pay damages of 100 crores to the Petitioners for damage to their brand and reputation and loss of good will;

j) Pass such other or further order as this Hon'ble Court may deem fit in and proper in the circumstances of the case.

AND FOR THIS KINDNESS THE PETITIONER AS IN DUTY BOUND SHALL EVER PRAY

Karuna Nundy
With Rahul Narayan, Ruchira Goel,
Ragini Nagpal, Utsav Mukherjee,
Abhay Chitravanshi, Shashwat Goel

ADVOCATES FOR THE PETITIONER

B-1/33A, Top Floor, HauzKhas
New Delhi-110016

Filed on:-**28 .05.2020**