2025:DHC:11874

$~J1

* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

Reserved on: 31st May, 2025
Pronounced on: 24th December, 2025
Uploaded on: 24th December, 2025

\+ **CS(COMM) 193/2019 & I.As. 5399/2019, 11497/2019, 18216/2019, 15451/2021, 31775/2024**

COLGATE PALMOLIVE COMPANY & ANR. ..... Plaintiffs

Through: Mr. Saif Khan Mr. Achuthan Sreekumar, Mr. Prajjwal Kushwah Ms. Imon Roy Mr. Achyut Tiwari Ms. Kanupriya Chawla, Mr. Swastik Bisarya Mr. Rohil Bansal Mr. Shivang Sharma, Advs.

versus

NIXI & ANR. ..... Defendants

Through: Ms. Akshita Jain, Advocate for D-1 (M-9990526912).

Mr. Darpan Wadhwa; Mr. Mrinal Ojha; Mr. Debarshi Dutta; Mr. Arjun Mookerjee; Ms. Nikita Rathi; Ms. Jewel Bhateja, Mr. Nikhil Gupta; Mr. Yogesh Singh, Mr. Shivam Tiwari, Mr. Anmol Dhindsa, Advs for D-3.

Mr. Danish Faraz Khan, Mr. Abhigyan Siddhant and Mr. Rahul Sharma, Advocates for UOI with Mr. Tanmay Nirmal, Manager legal.

Mr. Tentu Satyanarayan, Director (Legal), UIDAI & Mr. Tanmaya Nirmal, Deputy Manager (Legal & Policy), UIDAI (M-9899113033).

Mr. Kushagra Goel, Mr Lovesh Goel, Ms. Tanya Singhal, Advs. for D-7.

2025:DHC:11874

Mr. Akshay Goel, Mr. Shivam Narang &
Mr. Lalit Kashyap, Advocates
SI Prince Kumar, PS Hauz Khas.
Mr. Sunil Gautam, SO, UIDAI.
Mr. Nishant Gautam (CGSC), Mr. Vardhman Kaushik and Mr. Prithviraj Dey, Advs. for MEITY.
Mr. C.M. Lall, Sr. Adv. with Mr. Nirupam Lodha, Mr. Kshitij Parashar, Ms. Vanshika Thapliyal, Ms. Ananya Mehan, Advs. for Verisign Inc.

CORAM:
JUSTICE PRATHIBA M. SINGH

JUDGMENT

Prathiba M. Singh J.,

Sr. No.	INDEX	Para No.
I.	BACKGROUND	1-7
II.	CS(Comm.) 193/2019 with I.A. 5399/2019, 11497/2019, 31775/2024 (under Order XXXIX Rule 1&2 of CPC)	8-11
III.	PROCEEDINGS IN THE SUIT	12-27
IV.	COMMON ISSUES ARISING IN THE BATCH MATTERS (a) Investigation of financial frauds and role of banks. (b) Assistance from Banks to Law Enforcement Agencies. (c) Mismatch of payment details – Beneficiary Bank Account Name Look-Up Facility. (d) Enforcement of orders - appointment of Grievance Officers by DNRs. (e) Privacy Protect feature.	28-78

V.	**STAND OF THE PARTIES** (A) ICANN – Internet Corporation on Assigned Names and Numbers (B) GoDaddy (C) Hosting Concepts (D) Newfold Digital Inc. (E) Verisign (F) Registry Services (G) Meity *(i) Response received from ICANN* *(ii) Response received from HIOX LLC* *(iii) Response received from CERT-IN* *(iv) Response received from Cyber Law and E -Security Division, Meity* *(v) Response Received From NIXI* *(vi) Response Received From NPCI* (H) MHA (I) Delhi Police (J) Submissions on behalf of the Plaintiffs in the batch matters	**79- 162**
VI.	**ANALYSIS AND FINDINGS** **PREVENTION OF FINANCIAL FRAUDS** **ISSUE I: WHAT ARE THE OBLIGATIONS AND LIABILITIES OF A DNR IN RESPECT OF AN ALLEGED INFRINGING DOMAIN NAME REGISTERED WITH THE SAID DNR? AND WHETHER THE SAME ARE SUFFICIENT FOR PROTECTING THE INTELLECTUAL RIGHTS OF THIRD PARTIES?** *a. Domain Name System.* *b. Role of Registry Operators: ICANN-Registry Agreement.* *c. Role Of DNRs: Registrar-Accreditation Agreement.* *d. Nixi - Registrar Accreditation Agreement.*	**163-262**

	e. Privacy Considerations Vis-À-Vis Disclosure Obligations. *f. New Registration Data Policy.* *g. Modus Operandi Of The Registrants Of Infringing Domain Names.* **ISSUE II: WHAT MEASURES MAY BE DIRECTED BY THE COURT TO BE IMPLEMENTED BY THE DNRS AND REGISTRY OPERATORS TO SAFEGUARD THE TRADEMARK RIGHTS OF THE PLAINTIFFS?** *a. Rights of Trademarks Owners in Domain Names.* *b. Responsibilities and Duties of Registry Operators And DNRs.* *c. Measures Implemented By DNRs And Registry Operators.* **ISSUE III: WHAT MEASURES MAY BE DIRECTED BY THE COURT AGAINST DNRS WHO REFUSE TO COMPLY WITH THE COURT ORDERS?** *a. Intermediary obligations of due diligence and safe harbour protection.* *b. Dynamic And Dynamic + Injunctions.*	
VII.	**SUMMARY AND CONCLUSIONS**	**263-282**
VIII.	**DIRECTIONS** (A) Directions to DNRs and Registry Operators. (B) Directions to the Government. (C) Directions qua grant of '***Dynamic*** +' injunction. (D) Directions to Banks.	**283**
IX.	**RELIEFS IN THE SUIT**	**284-292**
X.	**SUMMARY ADJUDICATION**	**293-302**
XI.	**I.A. 15451/2021 (UNDER ORDER I RULE 10 OF CPC)**	**303-304**

This hearing has been done through hybrid mode.

I. BACKGROUND

1. What is a domain name? A domain name is the address of a business/individual/entity on the internet. The website built on the domain name is like a shop being built at the physical address of a business. In the internet age, domain names/websites form the ***`Online Soul'*** of a business. In order to maintain the distinctive nature of the business, domain names are usually registered using the brand name, house name or trade mark with which the business is associated. Any misuse of the same by registration of fraudulent domain names and creation of fake websites results in erosion of the integrity and goodwill of the business house and name, as also leads to consumer deception.

2. This batch of several commercial suits have been filed by various trademark owners seeking injunctions against misuse of their trademarks through registration of domain names by unknown persons. These domain names consist of either the full trademark or a distinctive part of the trademark or the brand name and are being used for illegitimate means in order to derive monetary benefits. The domain names that are registered are being misused in various forms such as:

(i) Registration of the domain names posing themselves as the Plaintiffs and collecting money under the garb of offering jobs, dealerships, franchisees, etc. The infringing domain name is used to create a website that hosts almost identical or similar content as that of the Plaintiffs' website. In some infringing websites similar logos or marks as that of the Plaintiffs'

are used along with misleading or deceptive information thereby enticing the general public into making payments through digital transactions into bank accounts which are not connected to the Plaintiffs.

(ii) Further, the infringing domain names are being registered for the purpose of hosting websites where counterfeit and pass-off products are being offered for sale or have been sold.

(iii) Fraudulent domain names are being used to host websites for providing services posing as the Plaintiffs.

3. The suits were instituted in respect of certain infringing domain names, with the concerned Domain Name Registrars (DNRs) impleaded as parties, as the identity of the Registrant could not be verified from the WHOIS records. The WHOIS details disclosed largely fictitious or incomplete particulars, with the sole contact point being an email address that does not disclose the identity of the Registrant. The DNRs possess only this limited information, and the remaining data provided at the time of registration such as addresses and mobile numbers is typically inaccurate. In the absence of any robust verification mechanism, even the email IDs used for registration are often created through temporary mobile numbers or public places such as cyber cafés, and BSI data frequently indicates that such Registrants are based on foreign shore. Consequently, obtaining the email address alone is insufficient, and it becomes exceedingly difficult to identify or trace the actual individual or entity responsible for registering the impugned domain name.

4. In cases where the bank account details are provided for the purposes of collecting money, a separate enquiry is required to be launched against the person

who has opened this bank account. On most occasions they are opened using mobile numbers which are again untraceable, or by way of the PAN card or Aadhar card which may be fake. The next level of enquiry then moves to the mobile number and the telecom service provider who usually collects some documents. However, the address etc., are again not traceable.

5. In effect, therefore, by registering domain names using a well-known mark or a registered trademark, a whole network is built only to deceive innocent and gullible consumers and members of the public. The bank account is operated for a temporary period and after the money is collected the same is withdrawn and even before the trademark owner is able to take action, the bank account is almost empty. Thereafter, even after the Court grants an interim injunction against the infringing domain names, there are further domain names/ websites registered and opened which follow the same pattern as described above. The whole gamut of fraudulent transactions and cyber fraud is being committed by those unknown persons and entities merely by registering infringing domain names and hosting websites that are misleading and containing deceiving content.

6. Thus, various issues arise for adjudication in these matters which are not limited to the present suit but are systemic issues which need to be addressed with significant changes and measures to be implemented by different stakeholders in the system. At the interim stage, for any effective injunction order to be passed, directions would be required to be issued to –

a. **Domain name registrants** – Person registering the domain name;

b. **Domain name registrars (DNRs)** – Entity enabling the registration of the domain name;

c. **Domain name Registry** – The Registry under which the DNR operates;

d. **ICANN** – Internet Corporation on Assigned Names and Numbers – the overall regulator of the Internet;

e. **Banks** – where the bank accounts are opened by the infringers;

f. **Reserve Bank of India** – Banking regulator which had to take steps to curb fraudulent activities through banking channels;

g. **Telecom service providers** – companies which provide SIM cards and associated telecom services

h. **MeiTY and DoT** – Ministries which oversee the access to the internet in India and also regulate the internet/telecom service providers

i. **Law Enforcement Agencies** – Police and other investigating agencies

7. In this batch of suits, the protection of the brand names, trade marks etc., is not only for the purpose of protecting the Intellectual Property and goodwill of businesses but to also to take effective steps against the large-scale cheating and deception of innocent consumers and users who are suffering huge losses due to misuse of trade marks and brand names on fraudulent domain names/websites.

II. CS(Comm.) 193/2019 with I.A. 5399/2019, 11497/2019, 18216/2019, 31775/2024 (under Order XXXIX Rule 1&2 of CPC)

8. The Plaintiff No.1 - Colgate Palmolive Company, a company incorporated in the State of Delaware, United States of America, and by Plaintiff No. 2 – Colgate Palmolive (India) Limited, a company registered in India under the

Indian Companies Act, 1919, have filed the present suit seeking, *inter alia,* permanent injunction and damages in respect of infringement of its various intellectual properties, including the trademark "*COLGATE*", copyright in the labels and packaging of its various products, passing off, rendition of accounts and delivery up. The reliefs sought in the present suit are as under:

> *"a) An order directing Defendant No. 1 to block the domain being operated by the Defendant No. 2 or transfer the same in the name of the Plaintiff No. 2, and to divulge the complete details of the Registrant(s) of the Defendant No. 2 to the Plaintiff No. 2, so as to stop this fraud immediately and enable the Plaintiffs to take necessary actions against the actual perpetrators of the said fraud; and*
>
> *b) An order of permanent injunction restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf from using the registered trademarks of the Plaintiffs in any manner whatsoever.*
>
> *c) An order of permanent injunction restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf from using the copyright of the Plaintiffs in the stylized representation of their marks in any manner whatsoever.*
>
> *d) For an order of permanent injunction restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf,*

from using the trademarks of the Plaintiffs and the brand name COLGATE PALMOLIVE as mentioned hereinabove being an obvious and fraudulent imitation of the Plaintiffs' website and the letter-heads to pass themselves off as the employees of the Plaintiff No. 2; and

e) For an order of permanent injunction restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf, from using the trademarks of the Plaintiffs and the brand name COLGATE PALMOLIVE as mentioned hereinabove being an obvious and fraudulent imitation of the Plaintiffs' website and the letter-heads to pass themselves off as the employees of the Plaintiffs, resulting in dilution and tarnishment of the well-known trademarks of the Plaintiffs: and

f) An order of delivery up of all infringing material (tangible and/or intangible), if any to the Plaintiffs for purposes of destruction and/or erasure; and

g) An order for rendition of accounts of profits fraudulently and illegally earned by the Defendant No. 2 on account of the fraudulent, illegal and infringing activities of the Defendant No. 2 and a decree for the said amount so found be returned to those from whom the said amount has been fraudulently earned; and

h) An order for damages in the sum of Rs.2,00,05,000/- in favour of the Plaintiff and against the Defendant No. 2 on account of the unauthorized use of the well-known trademarks of the Plaintiffs by the Defendant No. 2 and a decree

for the said amount be passed in favour of the Plaintiffs; and

(i) An order for costs of the proceedings against the Defendant No. 2 and in favour of the Plaintiffs; and

(ii) Any other Order(s) as this Hon'ble Court may deem fit and proper in the facts and circumstances of the case."

9. The present suit is part of a batch of matters relating to domain names being registered by unknown third parties infringing trademark rights of various brand owners and implementation of Court orders by different concerned entities including the Domain Name Registrars (hereinafter "*the DNRs*").

10. The Plaintiff has also initially preferred ***I.A. 5399/2019*** under Order XXXIX Rule 1 & 2 read with Section 151 of the Code seeking, *inter alia, ad-interim ex-parte* injunction restraining various websites/entities engaged in infringement of Plaintiffs' copyright, trademarks etc. The reliefs sought in the application are as under:

"a) An ex-parte ad-interim order directing Defendant No. 1 to block the domain being operated by the Defendant No. 2 or transfer the same in the name of the Plaintiff No. 2, and to divulge the complete details of the Registrant(s) of the Defendant No. 2 to the Plaintiff No. 2, so as to stop this fraud immediately and enable the Plaintiffs to take necessary actions against the actual perpetrators of the said fraud; and

b) An ex-parte ad-interim order directing State Bank of India to block the Account Number — 32268573333 located at the Branch having the IFSC

Code — SBIN0008079, and to share the complete details of the said Account Holder to the Plaintiff No. 2, so as to stop this fraud immediately and enable the Plaintiffs to take necessary actions against the actual perpetrators of the said fraud

c) The ex-parte ad-interim order granted hereinabove as prayed for in paragraph 42(a) and (b) may also kindly be passed against the Defendant No. 1; and

d) For an order of ex-parte ad-interim injunction restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf from using the registered trademarks of the Plaintiffs in any manner whatsoever; and

e) For an order of ex-parte ad-interim injunction the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf from using the copyright of the Plaintiffs in the stylized representation of their marks in any manner whatsoever; and

f) For an order of ex-parte ad-interim injunction restraining restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf, from using the trademarks of the Plaintiffs and the brand name COLGATE PALMOLIVE as mentioned hereinabove being an obvious and fraudulent imitation of the Plaintiffs' website and the letter-heads to pass themselves off as the employees of the Plaintiff No. 2; and

g) For an order of ex-parte ad-interim injunction restraining restraining the Defendant No. 2, its partners / proprietor, principal officers, servants, agents, representatives, dealers and all others acting for and on its behalf, from using the trademarks of the Plaintiffs and the brand name COLGATE PALMOLIVE as mentioned hereinabove being an obvious and fraudulent imitation of the Plaintiffs website and the letter-heads to pass themselves off as the employees of the Plaintiffs, resulting in dilution and tarnishment of the well-known trademarks of the Plaintiffs; and

h) Any other Order(s) as this Hon'ble Court may deem fit and proper in the facts and circumstances of the case."

11. Similar applications have been preferred by the Plaintiffs from time to time upon becoming aware of additional domain names. This Court *vide* order dated 12th April, 2019, had passed an order of interim injunction restraining the concerned Defendants, who are Registrants of the infringing domain names, from infringing the Plaintiff's marks. By way of the present judgement the Court shall dispose off the present suit and the pending applications.

III. PROCEEDINGS IN THE SUIT

12. The grievance in the present plaint is that there are various domain names and websites, registered/hosted by unknown individuals who have started using the mark "*COLGATE*", "*COLPAL*", "*COLGATE PALMOLIVE*" and depicting various products bearing said marks. In the present case, till date, there are 7 infringing domain names which have been identified:

Domain Names			
Sr. No.	***Link (do not put https/www)***	***DNR***	***Whether the domain is currently part of the common pool and available for registration? (Yes / No)***
1.	www.colgatepalmoliveindia.in	GoDaddy.com, LLC	No
2.	www.colgatepalmolive.in	GoDaddy.com, LLC	No
3.	www.colpal.in	GoDaddy.com, LLC	No
4.	www.colgateindia.com	CSC Corporate Domains, Inc.	No
5.	www.hrcolgatepalmolive.com	-	Yes
6.	www.colgateindia.in	GoDaddy.com, LLC	No
7.	www.colgatepalmolive.work	GoDaddy.com, LLC	No

13. Initially, the present suit was filed in respect of the domain name '***colgatepalmoliveindia.in***' which was being utilised by one Mr. Vishal Sharma @ Aditya, whose identity could not be confirmed, for sending emails to unsuspecting members of public for job interviews in the name of the Plaintiffs. The said individual fraudulently portrayed himself as the head of Humar Resources Department of the Plaintiffs and was soliciting money from the targeted persons for the fake interviews. In respect of the same, the following emails were being used:

(i) hr@colgatepalmoliveindia.in

(ii) vishal@colgatepalmoliveindia.in

(iii) info@colgatepalmoliveindia.in

14. The Plaintiffs were aggrieved by the fact that the WHOIS details of the said infringing domain name had been masked by the concerned DNR, which prevented the Plaintiff from initiating proceedings against the actual perpetrator of the frauds. The Plaintiffs are stated to have also filed criminal complaints against the said individual in respect of the frauds that were brought to their attention by the innocent/targeted individuals.

15. The present suit was heard on 12th April, 2019, and summons was issued to the Defendants. The Court had also considered the ***I.A. 5399/2019*** seeking interim injunction against the infringing domain names. The Court after considering the submissions made on behalf of the Plaintiffs and perusing the relevant documents placed on record was convinced that a *prima facie* case had been made out by the Plaintiffs for granting *ex-parte* injunction in favour of the Plaintiffs. The relevant portion of the said order reads as under:

> *"3. The case of the plaintiff is that it is in the business of oral care products in India since 1937. It is pleaded that the plaintiff's products enjoy tremendous goodwill and reputation throughout India. Since its inception plaintiffs have been continuously and consistently using the trademark and trade name COLGATE and also the domain name. In addition to the common law rights that have accrued to the plaintiffs by virtue of the aforesaid facts, it is also the registered proprietor of several COLGATE-formative trademarks in India in relation to various goods across various classes. It is further stated that the plaintiffs' trademark COLGATE over a long period of time has gained an unparalleled reputation and goodwill and*

has acquired the status of a well known trademark.

4. Defendant No.1 is the National Internet Exchange of India which is a Not-for-Profit company under section 25 of the Indian Companies Act, 1956. It was formed with the objective of facilitating improved internet services in the country. Defendant No.2 is the website called www.colgatepalmoliveindia.in which is operated by unknown persons whose identity and particulars are currently unknown. All that is known is the defendant is in fact one Vishal Sharma which could very well be a fake identity, is sending out emails using the said IDs hr@colgatepalmoliveindia.in, vishal@colgatepalmoliveindia.in and info@colgatepalmoliveindia.in and inviting innocent and unsuspecting members of the public for job interviews in the name of the plaintiff No.1, Colgate Palmolive India, while soliciting money deposits from the said prospective interviewees. It is submitted that the exact constitution and other details of defendant No.2 are not known. Plaintiffs were first informed of the infringing activities of the defendant through the emails and messages received from the supportive and sympathetic members of the general public who informed the plaintiff No.2 of the actions of defendant No.2. Further, defendant No.2 has also been sharing the account details of an SBI account and Axis Bank account where it has been soliciting money from unsuspecting members of the public as security deposit for the said fake interview.

5. Plaintiff has also taken steps to file a criminal complaint against the perpetrators of the crime. FIR is yet to be registered. It is pleaded that this is a clear indication of the attempts of defendant No.2 to pass off themselves as the HR of the plaintiff No.2. This is also indicative of the

intention of defendant No.2 to unjustly enrich their pockets at the expense of the general public and the plaintiffs while committing this act of fraud, misrepresentation and cyber-squatting.

6. Plaintiff has made out a prima facie case. Balance of convenience is also in favour of the plaintiffs and against the defendants. Defendant No.1 is directed to forthwith block the domain names hr@colgatepalmoliveindia.in, vishal@colgatepalmoliveindia.in and info@colgatepalmoliveindia.in being operated by defendant No.2. Defendant No.2 will also thereafter transfer the domain names in favour of plaintiff No.2. Defendant No.1 will also disclose the details of the persons who have opened the aforesaid domain name.

7. State Bank of India is directed to block the account No.32268573333 IFSC Code SBIN0008079. 8. Learned counsel for the plaintiffs also states that apart from this account there is another account of Oriental Bank of Commerce being A/C No.13332413000935 IFSC Code ORBC0101333 and that a communication to this effect has been received from one of the victims that a fraud has been played by the defendants which is at page 677 of the list of documents. Oriental Bank of Commerce is also directed to block the aforenoted account. The banks will also inform the court details of the account holders of the aforenoted accounts."

16. On 6th May, 2019, an application filed by the Plaintiffs seeking certain typographical corrections in the order dated 12th April, 2019 was allowed by the Court in the following terms:

" This application is filed by the plaintiff seeking correction of the typographical error in the order dated

12.4.2019. On 12.4.2019 this court had directed as follows:-

> *"6. Plaintiff has made out a prima facie case. Balance of convenience is also in favour of the plaintiffs and against the defendants. Defendant No.1 is directed to forthwith block the domain names hr@colgatepalmoliveindia.in, vishal@colgatepalmoliveindia.in and info@colgatepalmoliveindia.in being operated by defendant No.2. Defendant No.2 will also thereafter transfer the domain names in favour of plaintiff No.2. Defendant No.1 will also disclose the details of the persons who have opened the aforesaid domain name."*

The said order should read as follows:-

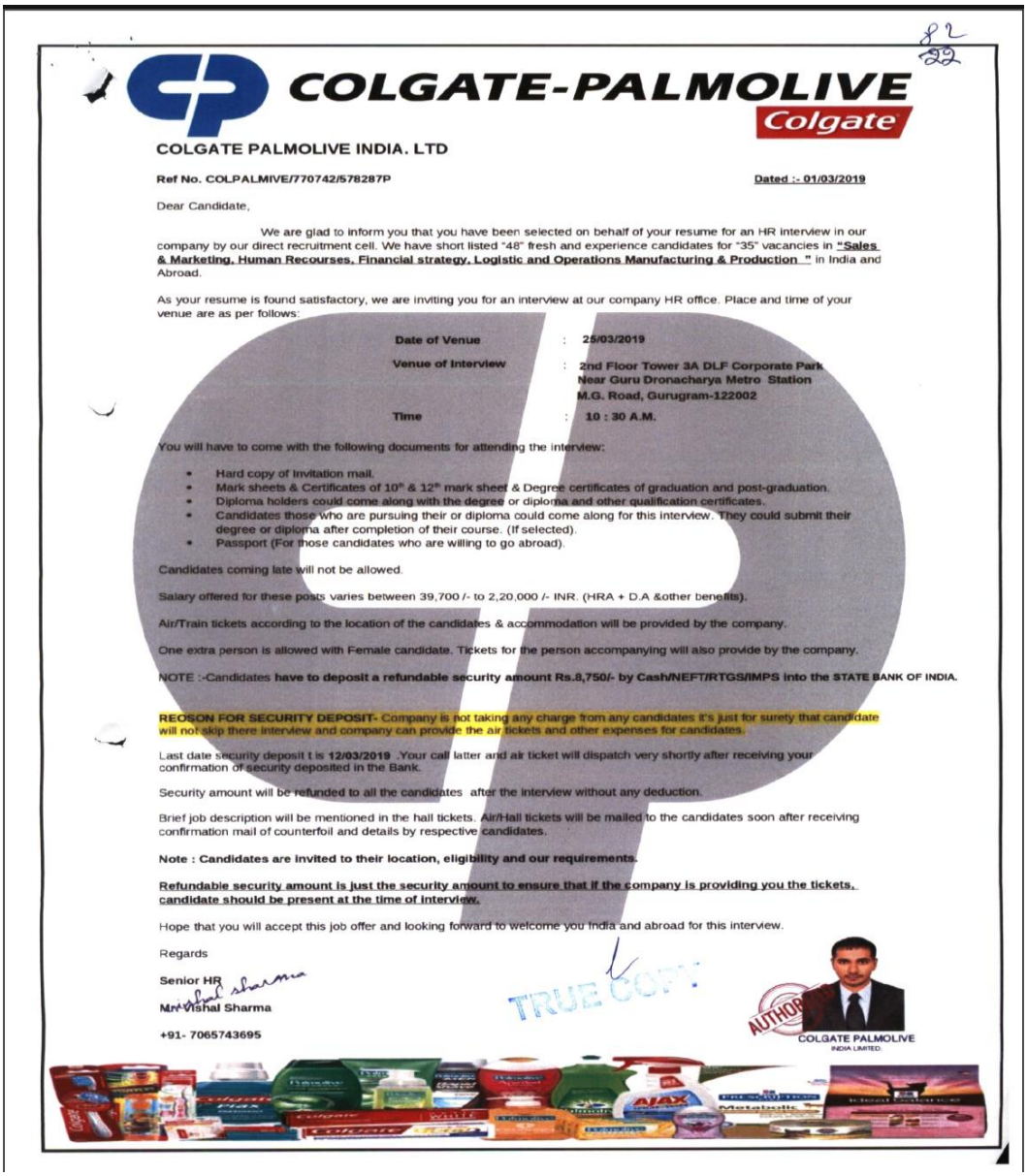
> *"6. Plaintiff has made out a prima facie case. Balance of convenience is also in favour of the plaintiffs and against the defendants. Defendant No.1 is directed to forthwith block the website and domain names www.colgatepalmoliveindia.in being operated by defendant No.2. Defendant No.2 will also thereafter transfer the domain name in favour of plaintiff No.2. Defendant No.1 will also disclose the details of the persons who have opened the aforesaid domain name."*
>
> *Application is allowed as above."*

17. In addition to the above, the Court *vide* various orders dated 15th May, 2019, 23rd August, 2019, 27th September, 2019, 24th December, 2019, 20th

October, 2023, and 26th June, 2024 has impleaded and granted interim injunction against infringing domain names as also the corresponding DNRs and/or banks.

18. On 21st November, 2019, the Court had heard the parties on the prayer of the Plaintiffs to impleaded GoDaddy.com LLC (hereinafter "*GoDaddy*") one of the DNRs of the infringing domain names in the present case. It was submitted by the Plaintiffs that although GoDaddy has complied with the directions of the Court in respect of blocking of the infringing websites, the Plaintiffs are aggrieved by the laxity of the Defendant No. 1 - National Internet Exchange of India (hereinafter "*NIXI*") in implementing its policy for collection of details of the Registrant by the DNRs. The Court permitted impleadment of GoDaddy has party to the present suit considering the same to be a necessary party for adjudicating the issues raised herein. Further, NIXI was also directed to file an affidavit as to whether the terms and conditions of the agreements with the DNRs warrants collection of information from the Registrants.

19. On 24th December, 2019, the Plaintiff had sought interim relief against another infringing domain name and the Court was informed that the same fake interview letter with Plaintiff's letter head was being used *albeit* this time by a person with different name. However, the photograph on the said letter remains the same as is seen in earlier fraudulent letters. The said letter is extracted hereunder for ease of reference:



COLGATE-PALMOLIVE

Colgate

COLGATE PALMOLIVE INDIA. LTD

Ref No. COLPALMIVE/770742/578287P

Dated :- 01/03/2019

Dear Candidate,

We are glad to inform you that you have been selected on behalf of your resume for an HR interview in our company by our direct recruitment cell. We have short listed "48" fresh and experience candidates for "35" vacancies in **"Sales & Marketing, Human Recourses, Financial strategy, Logistic and Operations Manufacturing & Production "** in India and Abroad.

As your resume is found satisfactory, we are inviting you for an interview at our company HR office. Place and time of your venue are as per follows:

Date of Venue : **25/03/2019**

Venue of Interview : **2nd Floor Tower 3A DLF Corporate Park Near Guru Dronacharya Metro Station M.G. Road, Gurugram-122002**

Time : **10 : 30 A.M.**

You will have to come with the following documents for attending the interview:

- Hard copy of Invitation mail.
- Mark sheets & Certificates of 10th & 12th mark sheet & Degree certificates of graduation and post-graduation.
- Diploma holders could come along with the degree or diploma and other qualification certificates.
- Candidates those who are pursuing their or diploma could come along for this interview. They could submit their degree or diploma after completion of their course. (If selected).
- Passport (For those candidates who are willing to go abroad).

Candidates coming late will not be allowed.

Salary offered for these posts varies between 39,700 /- to 2,20,000 /- INR. (HRA + D.A &other benefits).

Air/Train tickets according to the location of the candidates & accommodation will be provided by the company.

One extra person is allowed with Female candidate. Tickets for the person accompanying will also provide by the company.

NOTE :-Candidates **have to deposit a refundable security amount Rs.8,750/- by Cash/NEFT/RTGS/IMPS into the STATE BANK OF INDIA.**

REOSON FOR SECURITY DEPOSIT- Company is not taking any charge from any candidates it's just for surety that candidate will not skip there interview and company can provide the air tickets and other expenses for candidates.

Last date security deposit t is **12/03/2019** .Your call latter and air ticket will dispatch very shortly after receiving your confirmation of security deposited in the Bank.

Security amount will be refunded to all the candidates after the interview without any deduction.

Brief job description will be mentioned in the hall tickets. Air/Hall tickets will be mailed to the candidates soon after receiving confirmation mail of counterfoil and details by respective candidates.

Note : Candidates are invited to their location, eligibility and our requirements.

Refundable security amount is just the security amount to ensure that if the company is providing you the tickets, candidate should be present at the time of interview.

Hope that you will accept this job offer and looking forward to welcome you India and abroad for this interview.

Regards

Senior HR

Mr. Vishal Sharma

+91- 7065743695

TRUE COPY

AUTHORISED SIGNATORY

COLGATE PALMOLIVE INDIA LIMITED

20. Considering the above, the Court had directed the additional infringing domain name to be blocked by the concerned DNR, and the respective bank accounts linked to the said domain name were also directed to be freezed.

21. Thereafter, the Plaintiff had preferred an application under Order I Rule 10 of CPC for impleadment of one Ms. Ruksar, Mr. Mohd. Safik, Mr. Rohit Nanda, and Mr. Naresh. The said application was considered on 16th February,

2021 and the same was allowed. Summons was issued to the newly impleaded defendants on the same date.

22. On 15th July, 2022, notice was issued in the ***I.A. 15451/2021*** filed by GoDaddy seeking deletion from the array of parties. Further, the ***I.A. 6069/2022*** filed by the Defendant No. 7 – Mr. Rohit Nanda also seeking deletion from the array of parties on the ground that one of fraudulent bank accounts in the present case had been opened using his credentials by some unscrupulous persons. In this regard, Mr. Nanda had stated to have also filed a police complaint with P.S. Haus Khas, New Delhi, which had been investigated *vide* DD No. 56A dated 1st November, 2021. In addition to the above, the Court was informed by the Plaintiff that it has filed a complaint with the Cyber Crime Unit, Special Cell in respect of the same. Considering the same, the Court was of the opinion that a larger fraud is being perpetuated by misusing the trademarks of the Plaintiffs. Accordingly, the Court had directed the status report of the Cyber Crime Unit, Special Cell to be placed on record. The relevant portion of the order dated 15th July, 2022 reads as under:

> *"5. This is an application filed by the defendant no. 7-Mr.Rohit Nanda seeking his deletion from the array of parties. In support of his prayer, the defendant no. 7 has placed a copy of the DD No. 56A dated 01.11.2021 of the Police Station Hauz Khas, New Delhi, which reads as under:-*
>
> *"**DD No 56A, dated 01-11-2021, PS Hauz Khas, ND***
> *Sir,*
>
> *On date 01-11-2021, a complaint regarding*

opening the forge account (bearing No. 13461000001796) in the Hauz Khas Branch of Punjab and Sind bank and fraudulent activities committed using this account was received in PS Hauz Khas vide DD no 56A. The above account is in the name of Rohit Nanda S/o Rajender Kumar R/o F- 206, Block -F, Pandav Nagar, Shakarpur, Delhi 110092. Complainant Rohit Nanda stated in his complaint that someone has opened the above forge account in his name and he had no information regarding opening of account or any activity associated to it.

An inquiry has been conducted in this regard and ***it has been found that the person who opened the above mentioned account has used forged identification proofs to open the account and he is not the same person as the complainant Rohit Nanda. It has been verified that the Identification proofs including Aadhar and PAN card and signature of alleged person used for opening the above mentioned forged account do not match the Aadhar and PAN card and Signature of the complainant Rohit Nanda. Biometrics used for opening the forged account have also been verified and found to be different from that of the complainant Rohit Nanda. Also, the photograph of the person who opened the forged account, does not match with Photographs of the complainant Rohit Nanda.***

Based on the Inquiry, it can be concluded that the complainant has no association with the above mentioned forged account or any activities related to that account. Name and

address of complainant Rohit Nanda S/o Rajinder Kumar has been misused by the alleged persons"

*4. **A reading of the above shows a very alarming state of affairs. A bank account has been opened in the name of the defendant no. 7, which the Police claims, was opened by using a forged Aadhaar and PAN Card; neither the biometrics used were those of the applicant; nor were his photographs used for the opening of the bank account.** The report, however, does not state that based on this inquiry what further action has been taken against the bank, its officials and what efforts have been made to find out the identity of the person who opened this bank account.*

[…]

*8. **A perusal of the order of this Court dated 12.04.2019 and the report from the Police Station, Hauz Khas referred hereinabove shows a larger fraud being perpetuated by misusing the trademarks of the plaintiffs.** The learned counsel for the plaintiffs submits that a complaint in this regard has been filed by the plaintiff, which is pending investigation with the Cyber Crime Unit, Special Cell.*

9. It is felt necessary that a Status Report regarding the investigation carried out by the Cyber Crime Unit, Special Cell be called for."

23. Further to the direction passed in the above order, on 12th September, 2022, the status report had been placed on record, as per which, the valid Aadhar Card and PAN card had been used for opening the bank account. However, the

Defendant No. 7 – Mr. Nanda insisted that he had no connection with the same and that the biometrics provided for opening the account differ from his. Accordingly, the Court issued notice to the Unique Identification Authority of India (hereinafter "*UIDAI*") and directed the ld. CGSC to seek instructions from the Income Tax Department in respect of the PAN account used for opening the account.

24. The matter was next heard on 13th September, 2022, on which date it was brought to the Court's attention by the ld. CGSC appearing on behalf of UIDAI, that two Aadhar cards have been issued having same name, father's name and address. However, the other details are different. Accordingly, in view of Section 33 of the Aadhar (Targeted Delivery of Financial and other Subsidies, benefits and Services) Act, 2016, the Court after taking consent of Mr. Rohit Nanda, directed UIDAI to place the details linked with the two Aadhar cards in a sealed cover before the Court on the next date. The said direction was reiterated *vide* order dated 10th May, 2024. Further, *vide* order dated 31st May, 2025, the Defendant No. 7 – Mr. Rohit Nanda was deleted from the array of parties.

25. It is noted that *vide* order dated 20th October, 2022, the Court had granted interim relief in respect of some additional infringing domain names in the following terms:

> *"5. It is submitted by ld. counsel for the Plaintiff that previously various orders have been passed by the Court wherein the Court has injuncted such domain names as also the DNRs from transferring such domain names to any person in the future. He relies upon order dated 9th October, 2023 passed in Sony Interactive Entertainment Inc. v. Vikash Kumar [CS(COMM). 922/2022] wherein the*

Court held as under:

> *"13. At present, as Defendant 9 is the only DNR before this Court, Defendant 9 shall ensure that it does not allow registration, in favour of any person, for the domain name sonyplaystationstores.com. Mr. Raja expresses a doubt as to whether such an order could be passed citing, in that regard, my earlier decision in Snapdeal Private Ltd. v Godaddycom LLC. There is a clear distinction between that case and this. In that case, the order that was sought was a blanket injunction against any domain name having the string "snapdeal" having been registered. I had stated – and continue to hold that view – that such an injunction could not be granted, as the court could not, in advance, presume that every domain name which included "snapdeal" as a part would necessarily be infringing. Such a direction could only be passed in respect of domain names which are actually before the Court. 14. In the present case, the said situation does not arise, as the domain name in question is sonyplaystationstores.com which this Court has already held, in its order dated 23 December 2022 to be prima facie infringing in nature. 15. At this juncture, Mr. Khan points out that Defendant 8-Big Rock is also a domain name registrar (DNR) who is impleaded in the present proceedings. 16. Accordingly, this order shall also extend to Defendant 8."*

6. Accordingly, there shall be an injunction against the use of the domain name www.colgateindia.in. NIXI is also directed to ensure and give instructions that the following

domain names are not permitted to be offered for sale to any third party except the Plaintiff in the future. Insofar as GoDaddy is concerned, it shall lock and suspend as also not offer to any third party the following domain names:
i) www.colgatepalmoliveindia.in;
ii) www.colpal.in;
iii) www.colgateindia.com;
iv) www.hrcolgatepalmolive.com;
v) www.colgateindia.in."

26. The said order has been relied upon by the Plaintiffs to submit that similar reliefs may be granted for preventing the impugned domain names from falling back to common pool and becoming available for re-registration. This is countered by Mr. Darpan Wadhwa, ld. Sr. Counsel for GoDaddy has been challenged in appeal by GoDaddy.com LLC, and the said appeal being ***FAO(OS)(Comm) 14/2024*** titled ***Godaddy.Com LLC v. Colgate Palmolive Company and Ors.*** is still pending.

27. This present suit was heard along with the batch of suits raising similar issues. All parties were heard by the Court on several dates and finally on 31st May, 2025 the judgement was reserved in the present suit. However, before the Court considers the submissions of the parties in the present suit, it would be necessary to discuss the directions passed by this Court in respect of certain common issues which arise in the present batch of matters.

IV. COMMON ISSUES ARISING IN THE BATCH MATTERS

28. In ***CS(Comm) 475/2022*** titled ***Fashnear Technologies Private Limited v. Meesho Online Shopping Pvt. Ltd. & Anr. (hereinafter "Fashnear***

Technologies"), *vide* order dated 20th July, 2022 it was noted that these cases of fraudulent and infringing domain names/websites being operated for collecting large sums of money from unsuspecting customers are not one-off instances. Considering the suits already filed by various trademark owners, the Court was of the view that these matters should be heard together for a consolidated investigation. The relevant portion of the order dated 20th July, 2022 reads as under:

> "*11. It has also been brought to the notice of this Court that there are a number of cases before the Court where fraudulent domain names are being registered under the marks of well-known and established business houses and their brands. The said domain names are being used for hosting fraudulent websites with details of bank accounts under the garb of offering jobs, dealerships, franchisees, lucky draws, and various other illegal activities. The cases already before this Court, include the following:*
> *[…]*
>
> *12. In addition, ld. Counsels appearing before this Court today have informed the Court that there are other similar matters, pending before different benches of the IPD. The details of the said matters are as under:*
> *[…]*
>
> *13. Subject to the orders of Hon'ble the Judge-in- Charge (Original Side), all the above matters be listed before the same Bench****, as the investigation needs to be consolidated and comprehensive directions may be required to be issued to the police authorities, cyber cells, the various banks, National Payment Corporation of India, RBI, MHA etc.***

> *14. The Cyber Crime Unit, Special Cell, Delhi shall continue the investigation in these matters. Let a further status report be submitted in respect of the said investigation, on the next date of hearing.*
>
> *15. It is also made clear that in order to coordinate in obtaining data relating to various bank accounts and other details of the persons, who opened the fraudulent bank accounts for collecting the money from the customers, the Cyber Crime Unit is free to approach National Payments Corporation of India, as also, the concerned banks."*

29. Accordingly, the present suit along with the batch of suits raising similar issues were heard by the Court on 3rd August, 2022. The Court after hearing the parties, formulated the various issues for consideration in the present batch of matters. The relevant portion of the said order dated 3rd August, 2022 reads as under:

> *"2. The primary issue that arises in these cases is that the proliferation of these domain names has resulted in enormous damage to innocent and gullible members of the public, who have been led to believe that the websites hosted on some 'impostor' domain names, in fact belong to the actual brand owners. The facts which have emerged from these cases show clearly that innocent persons have been duped of crores of rupees due to registration of domain names consisting of well-known brands and trademarks.*
>
> *3. The second issue that has arisen in all these cases is that the persons registering these domain names, on most occasions, have masked their identities. This could be voluntarily done by the registrants themselves or due to features that are enabled by the domain name registrars (hereinafter "DNRs"), that provide bundled services when*

registering a domain name, such as privacy protect features and proxy domain services.

4. Third, even if such information is unmasked, the information being collected by the DNRs at the stage of registration of the domain name appears to be quite unsatisfactory inasmuch as even when Courts have directed the data relating to the registrants to be supplied to the Plaintiff, on most occasions, the details are fictitious and are not traceable. It has required several orders of Courts being passed, and investigations by police authorities as also Cyber Cells, to even trace the natural persons behind the said domain name registrations, through the telephone numbers and bank accounts through which payments may have been made for registering the domain names.

5. In this background, the Plaintiffs in these cases insist on blanket injunctions to be passed against the DNRs, injuncting them from registering any domain names consisting of the Plaintiff's marks and brands. On the other hand, the DNRs resist this prayer on the ground that the alphabets contained in these marks and names are such that there could be genuine

[...]
31. After hearing the submissions made today by various parties, this Court is of the prima facie opinion that the manner in which the present system is working is completely unsatisfactory. ***Whenever any domain name is registered which consists of a well-known mark or a registered brand name which the owner intends to protect, the remedies that can be availed of are either to seek remedies under UDRP or approach the Court. The sheer quantum and magnitude of domain names which are capable of being registered, especially by persons who***

intend to indulge in fraudulent activities would make it almost impossible for IP owners to avail of their remedies qua each and every domain name*. Especially in the case of marks which are well known, there ought to be a more efficient framework which needs to exist. Considering the large sums of money that are being fraudulently obtained from various unsuspecting customers, all due to the lack of an active mechanism identification of such fraudulent parties, it is clear to the Court that the following aspects need to be addressed in these matters:*

(i) The manner in which the details of the domain name registrants, can be verified by the DNRs, at the time of registration of domain names;

(ii) The manner in which the privacy protect feature and proxy servers are made available: whether it is only upon a specific registrant choosing the said option, rather than as a standard feature as part of a 'bundle';

(iii) If the owner of a well-known brand or a trademark contacts any DNR, the manner in which the data related to the registrant can be provided, without the intervention of a Court, or any governmental agency;

(iv) Whether the identity of the owner of a domain name, which consists of a registered trademark or a known brand can be verified at the time of registration itself;

(v) If a specific link could be provided by the CGPTDM, covering a list of well-known marks, maintained by the Registrar of the Trademarks, or declared by any Court of law, which can then be used for expedited blocking of domain names

consisting of such marks;

(vi) If there can be any agency that can be identified in India, such as NIXI, who can be made a repository of the data concerning the registrant, or an agency through which the data could be transmitted by the DNR, upon verification by NIXI, in case a trademark owner has a grievance against a specific domain name;

(vii) If any directions are issued to the DNRs, and the same are not implemented, the manner in which the implementation of the said orders can be ensured;

(viii) Since almost all domain names are registered only after payments are made through credit card, or other online payment methods or apps, is it possible, upon request by any identified agency, to provide the information relating to the person who has made the payment, to the trademark owners. This should be discussed in the aforementioned meeting to be held on 30th August, 2022.

32. The recommendations in respect of the above aspects, shall be given by DoT and/or MeitY. All these aspects shall also be dealt with by the specific affidavits, which shall be filed by the DNRs, who are offering their services in India.

33. If the DNRs are offering any other additional services by themselves, or through their affiliate / associate companies, such as web hosting, cloud services, etc., the said affidavits shall contain any additional data, or information, that the DNRs obtain in such cases, and if so, in what manner is this data stored with them."

Investigation of financial frauds and role of banks

30. On 3rd August, 2022, the Court was informed that the Cyber Crime Unit, Delhi Police has constituted a Special Investigation Team called the Intellectual Fusion and Strategic Operations (hereinafter "*IFSO*"), to look into the misuse of well-known marks in misleading domain names, website and URLs. Further, *vide* status report dated 3rd August, 2022 filed in ***Fashnear Technologies (supra),*** it was stated that out of the 28 suits pending in the batch, in 17 matters First Information Reports have been registered and pursuant to the orders passed by the Court similar investigations have been consolidated with the IFSO. Considering the scale of collection of monies and the necessity of cooperation from the banks, Telecom Service Providers (hereinafter "*TSP*") and Internet Service Providers (hereinafter "*ISP*") for gathering of information and better coordination, the Court had directed a joint meeting amongst the IFSO, the Delhi Police, the National Payments Corporation of India (hereinafter "*NPCI*"), the Indian Computer Emergency Response Team (hereinafter "*CERT-IN*"), DoT and MeitY.

31. On 14th September, 2022 the Court was informed about the status of the investigation being conducted by the IFSO in the batch matters. The status reports had been filed in 25 suits and Ms. Hetu Arora Sethi, ld. ASC had taken the Court through some of the said reports. It was observed by the Court that as per the status reports monies have been collected illegally by using the brand names, marks and business names of the Plaintiffs under the garb of offering distributorships, franchisees, employment etc. The said amounts are deposited in bank accounts opened in individual names but represented as belonging to the

Plaintiffs and are withdrawn almost instantaneously. However, the magnitude of the fraud being committed was still to be unearthed. Accordingly, it was directed that the investigation shall continue and further status report be filed by 1st December, 2022.

32. Further to the above directions, the Court was informed on 1st December, 2022 that in 6 out of 25 cases, chargesheets have been filed and in few cases arrests have also been made. However, in some cases since the victims were not found in Delhi, the investigation did not proceed further. The Court clarified that where the brand owners of the registered marks are located in Delhi or if any transaction has taken place in Delhi, the Cyber Cell, Delhi Police, may register the FIR and conduct investigation. The IFSO was also directed to file a consolidated status report within four weeks.

33. On 27th September, 2023, Ms. Sethi, ld. ASC had placed on record a consolidated status report dated 23rd September, 2023 and submitted that chargesheets have been filed in 10 cases. In addition to the same, in compliance with the directions passed on 16th August, 2023, a written note of arguments was placed on record detailing the challenges faced by the Cyber Cell, Delhi Police, in investigation of cases involving similar issues as present batch of matters. The challenges mentioned therein, in brief, are as under:

i. Delay by banks in replying to emails and information sought by the Cyber Cell.

ii. DNRs and intermediaries who are hosting the website not providing proper details of the Registrants in respect of cloud services and other services availed by them.

iii. Use of Voice Over Internet Protocol (hereinafter "*VOIP*"), Virtual Private Network (hereinafter "*VPN*"), etc. by fraudsters to avoid detection.

iv. Non-providing of information by Google even though fake websites have booked AdWords through Google Ads programme.

34. The Court had perused the written note of arguments and heard Ms. Sethi, ld. ASC before issuing notice to all the nominated counsels of all the banks, who have been nominated by the Delhi High Court, so as to evolve a method for ensuring that queries by the police authorities are replied to in a diligent and efficient manner, as it involves innocent customers being duped of substantial sums of money. Insofar as Google LLC was concerned, the Court directed it to nominate one official for communication with the Cyber Cell, Delhi Police and rendering necessary assistance.

Assistance from Banks to Law Enforcement Agencies

35. The ld. Counsels for various banks, including the RBI, had entered appearance on 24th November, 2023. The Court directed RBI to file an affidavit addressing any guidelines which may have been issued to the banks in respect of providing assistance to police authorities and complying with the directions of the Court. In addition, the banks present before the Court were directed to also file an affidavit as to the procedure followed by them to reply to queries of the police.

36. Ms. Sethi, ld. ASC had also pointed out to the Court that in a number of cases the ultimate accused is located in other States, making it difficult for the

Delhi Police to conduct investigation and prosecute the said accused person. Accordingly, observing that there is a need for co-ordination between the various Cyber Crime Cells in the country, notice was issued to the Ministry of Home Affairs (hereinafter "*the MHA*"). Further, the Joint Secretary, MHA was directed to hold a meeting on 20th December, 2023 between the Cyber Crime Cells of different States to deal with cases involving financial fraud done on the internet.

37. Pursuant to the above directions, a meeting was held with the banks by the RBI and the MHA, including the Director General of Police of some States. It was expressed by the Law Enforcement Agencies (hereinafter "*LEAs*") in the said meeting that the banks ought to expedite the process of providing of information. On 1st February, 2024 it was submitted by the ld. Counsels for the banks, that this issue has been taken cognizance of by the Indian Banks Association (hereinafter "*IBA*"). On behalf of RBI, a detailed Standard Operating Procedure (hereinafter "*SOP*") was placed on record along with affidavit dated 16th January, 2024, as per which strict deadlines have been fixed for banks to provide information to the LEAs, and the same are mandatory. The Court, after hearing the parties, and considering the SOP, directed the IBA to hold meetings of its sub-groups and sub-committees to ensure that all banks implement the SOP. Accordingly, notice was issued to IBA and it was directed to place on record its stand in respect of implementation of the SOP.

38. Thereafter, on 15th April, 2024, in terms of the above directions, an affidavit was filed on behalf of IBA. As per the same, there was an existing SOP dated 11th April, 2022 which was in operation as approved by the Central Intelligence Economic Bureau (hereinafter "*CIEB*"). However, pursuant to the

directions of this Court and the meetings held by RBI with the concerned stakeholders, another sub-group was created by IBA for updating the existing SOP. The updated SOP were also placed on record and the same were perused by the Court. The updated SOP directed appointment of nodal officers as Single Point of Contact, creation of a dedicated email account and publishing the details of the compliance officers on the websites. It also laid down timelines for providing information to the LEAs. It was submitted by the ld. Counsel for RBI that the said SOP would be shared with all the banks after the same are approved by CIEB and RBI. Accordingly, considering that the finalising of the SOP shall take further time, the Court had directed the banks to adhere to the timelines mentioned in the updated SOP placed on record. The process of finalising the said SOP was directed to be concluded by 30th May, 2024 and thereafter, the same were to be communicated to all the banks.

39. In addition to the above, the Court was also informed by the ld. CGSC, of a new agency established by the MHA *i.e.,* the Indian Cyber Crime Coordination Centre (hereinafter "*I4C*") with the following mandate:

> *"8. The Ministry of Home Affairs has rolled out the Indian Cyber Crime Coordination Centre (I4C) which has the mandate to develop effective coordination and cooperation amongst the LEAs of States/UTs and other stakeholders of cybercrime.*
>
> *9. The I4C provides two modes of reporting online cybercrime complaints. First mode is through "National Cybercrime Reporting Portal" (NCRP) website [www.cybercrime.gov.in] and the second mode is through National Cybercrime Toll-free Helpline No. 1930. The NCRP portal is designed for reporting all types of*

cybercrime including online financial crimes. The NCRP portal is composed of two components - one for citizen complaint reporting and another for the Police to monitor and act up on those complaints and access other resources. The portal allows victims of cybercrime to easily lodge their complaints without having to visit any police stations. The portal helps the States/UTs to monitor various types of cybercrimes originating both nationally and internationally and take necessary steps to curb them.

10. The Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) has been developed by I4C to integrate Law Enforcement Agencies (LEAs), banks, and financial intermediaries to take immediate action against financial cyber frauds. The system empowers both banks and the police by allowing them to share online fraud-related information in real-time, enabling them to take swift action. The system traces the flow of crime proceeds through the financial channels and aims to prevent the outflow by timely interventions. Without timely intervention, the outflow of the crime proceeds is not possible to stop in the financial system. All States/Union Territories (UTs) and 293 Banks and Financial Institutions have been onboarded to CFCFRMS so far for effective visibility and to take swift action on the movements of fraudulently reported amounts and mark lien or freeze the same within the financial channels by the Law Enforcement agencies. The Law Enforcement Agencies of all States/UTs take necessary actions on the complaints received online on the portal as per law. l4C, Ministry of Home Affairs has no intervention in the process.

12. The l4C has constituted seven Joint Cyber Coordination Teams (JCCTs) [as tabulated below] in consultation with the States/UTs on the basis of cybercrime hotspots/areas for effective coordination of Law

> *Enforcement Agencies. JCCT is mandated to achieve effective coordination among States/UTs for inter-state investigation assistance, intelligence-led operation, criminal profiling, data. Sharing, identification of suspects, real-time exchange of information, and cooperating on all other aspects of cybercrime and cyber threats. The JCCT is a regional grouping of States/UTs that can work together and also collaborate with the I4C, New' Delhi, broadly in the areas of being a knowledge and resources sharing platform to holistically tackle cybercrime."*

40. The Court was apprised on 2nd July, 2024 by the ld. Counsel for RBI that the updated SOP *qua* the process for providing information by the banks to the LEAs, has been finalised by IBA in consultation with the CIEB, and the same has been circulated to all banks *vide* email dated 3rd June, 2024.

41. On 21st December, 2024, the Court had considered the updated standard operating procedures issued by CEIB in respect of a request for information made by a LEA to be followed by the Banks. After hearing the parties the Court had passed certain directions. The relevant portion of the order dated 21st December, 2024 reads as under:

> *"5. The above discussion would show that insofar as the said SoP for sharing information with LEAs is concerned, the IBA has to ensure the implementation of the same by the banks, which has not yet been done.*
>
> *6. The banks contend today that the SoP is still not a binding document. Mr. Gupta, at this stage, submits that he would then have to seek instructions in the matter and apprise the Court as to whether the said SoP has actually been followed or not.*

> *7. Accordingly, issue court notice to Mr. Rajesh Kumar Gautam, ld. Counsel for Indian Bank Association (IBA) (M: 9811252434, email rajeshgautam@klmehta.net) in this matter for seeking instructions. Let an affidavit be filed on behalf of the IBA as to whether it has advised all the banks to ensure that the SoP is fully and strictly adhered to and also whether the same was circulated to all the banks or not.*
>
> *8. In addition, Mr. Gupta ld. Counsel shall also to take instructions from the banks he is representing about the implementation of the SoP.*
>
> *9. Both ld. Counsel for IBA and Mr. Gupta shall also seek instructions and file an affidavit on how much period is taken for freezing bank accounts after a Law Enforcement agency request and/or order of the Court is furnished to the banks."*

42. On 7th February, 2025 Mr. Sanjay Gupta, ld. Counsel had appeared and submitted that he would obtain instructions and file a report by the next date of hearing in respect of the implementation of the circular dated 30th December, 2024 by the banks represented by him. Further, insofar as the IBA is concerned, Mr. Rajesh Kumar Gautam, ld. Counsel had appeared through Video Conferencing and submitted that an affidavit has also been placed on record on behalf of the IBA in terms of the order dated 21st December, 2024.

43. Mr. Gautam, ld. Counsel had also handed across an email dated 3rd June, 2024 from the IBA which was sent to all banks, including public sector, private sector, foreign, co-operative and regional rural banks, enclosing the updated SOP for providing information to the LEAs. Thus, all banks have been advised to

follow the updated SOP for providing the information to LEAs within the time period and as per the manner prescribed therein.

Mismatch of payment details – Beneficiary Bank Account Name Look-Up Facility.

44. At this stage it is relevant to note that another significant issue that came to the attention of the Court on 14th September, 2022 *i.e.,* the mismatch of payment details whenever payments are made for purchase of domain names. As per the Plaintiffs, there is a mismatch between the actual name of the account holder as registered with the concerned bank and the name provided for billing to the DNR. It was submitted that there is currently no verification method to check if the name of the account holder is the same as the name entered at the time of purchase. The Plaintiffs prayed for directions to remedy this position and prevent innocent public from being duped by fraudulent domain name Registrants. The Court had directed the MeitY to consider the said issue in its meetings with the stakeholders as also directed NPCI to provide its views on the same.

45. On 1st December, 2022, the Court was of the view that this issue also ought to be considered by the Reserve Bank of India (hereinafter "*RBI*"). Accordingly, notice was issued to the ld. Standing Counsel/Nominated Counsel for RBI – Mr. Ramesh Babu M.R. The RBI was also directed to place its stand on record on this issue along with recommendations to remedy the same.

46. An affidavit dated 9th February, 2023 was handed over on behalf of RBI in compliance of the above directions. The stand of the RBI was that it has issued from time to time various guidelines in respect of payment through Real Time

Gross Settlement (hereinafter "*RTGS*") and National Electronic Fund Transfer (hereinafter "*NEFT*") modes, as also, in respect of mandatory compliances that are to be affected by the banks at the time of opening of accounts. However, it was stated that RBI has not issued any specific instructions advising banks to ensure that the name of bank account holder and the names in the billing details correspond to each other. Further in respect of the actions which can be taken by NPCI it was stated as under:

> *"10. It is submitted that Immediate Payment Service (IMPS), one of the modes of electronic fund transfer is operated by National Payments Corporation of India (NPCI).* ***NPCI has enabled the banks to offer beneficiary account validation functionality to confirm the beneficiary account name (as per bank CBS) and account status before making the transaction****. Banks need to ensure that they are equipped for providing this functionality and also necessary changes in their Bank application (net banking/mobile banking) User Interface (UI)/User Experience (UX) to enable this functionality to their customers in the transaction process flow.* ***Unified Payments Interface (UPI), which is also operated by NPCI offers the functionality wherein the customer can verify the beneficiary UPI ID/Virtual Payment Address (VPA) from the app thus providing a layer of protection to the remitter."***

47. It was further submitted by Mr. Ramesh Babu, ld. Standing Counsel for RBI, that it is mandatory to conduct KYC before opening of a bank account. However, the verification of the beneficiary account name is a functionality, introduced by the NPCI, is available with the banks and it is upon them to enable it. The Court, after considering the submissions of the parties as also the affidavit

of RBI, directed RBI to seek instructions whether RBI can issue guidelines making it mandatory for banks to match the beneficiary's name/ name in the billing details with the *account holder's name* and *not merely the account number*, whenever banks accepts online or offline payments.

48. The Court was informed on 27th March, 2023 *via* an affidavit sworn by the Assistant General Manager, Department of Supervision (Banking), RBI of the position of RBI *qua* making it mandatory to match beneficiary's name in the billing details with the account details before passing credit. The same is extracted hereunder:

> *"6. It is further submitted that Digital Payment products provides beneficiary name verification services which the originator can use to verify the name of the account to which funds are being transferred prior to initiating transfer. At present, the facility of beneficiary name lookup at the time of origination of transaction is available for UPI. RBI is exploring the feasibility for introduction of the aforesaid facility in other payment products such as RTGS, NEFT, IMPS etc both in online and off-line i.e. at the bank branch modes, and steps would be taken by RBI after taking into account technology, data privacy and other related issues.*
>
> *7. It is submitted that issuing guidelines making it mandatory for banks to match the beneficiary's name in the billing details with the account holder's name before passing on credit will make digital payments inefficient and result in a large number of returns. In view of the submissions made herein above, RBI is not in favour of issuing any guidelines making it mandatory for banks to match name before passing on credit."*

49. In view of the above position, RBI was directed to seek instructions as to the timelines, if any, for introduction and implementation of the ***beneficiary name lookup facility*** at the time of origination of transactions in cases of RTGS, NEFT and Immediate Payment Service (hereinafter "*IMPS*"), both in online and offline mode.

50. Accordingly, on 26th May, 2023, the Court was apprised, in terms of the previous order, that the ***'beneficiary name lookup facility'*** would be made operational by June, 2024. Thereafter, on 2nd July, 2024, an affidavit dated 2nd July, 2024 was handed across by the ld. Counsel for RBI, as per which, the ***'beneficiary name lookup facility'*** had been implemented in respect of IMPS. Further, it was stated that the banks would be advised by December, 2024 to extend the said facility to customers using RTGS and NEFT payment systems.

51. Further to the above, on 21st December, 2024 the ld. Counsel for RBI had handed across a press release dated 9th October, 2024, as per which, the 'beneficiary name lookup facility' has been implemented insofar as UPI and IMPS mode of payment in concerned. However, it was submitted by the ld. Counsel that a similar facility in respect of RTGS and NEFT was under testing and would be made available to the banks soon along with relevant guidelines for the same. Accordingly, the Court after considering the above submissions directed the RBI to expeditiously activate the said facility. The relevant portion of order dated 21st December, 2024 reads as under:

> *"13. Steps being taken by the RBI to for implementation of the said Beneficiary's Name Lookup Facility for RTGS and NEFT transactions are extremely crucial to prevent cyber fraud like the kind of fraudulent activity that are being dealt*

> *in this case. The RBI shall , without any delay, create the said facility referred to as, Beneficiary's Name Lookup Facility in terms of its affidavit and the press release dated 9th October, 2024 as also in terms of various previous orders of this Court. Delay in the implementation is likely to impact thousands of innocent consumers, who make payments without realising who is the beneficiary.*
>
> *14. Let the RBI expeditiously activate the said system of Beneficiary's Name Lookup Facility and inform the IBA and its member banks of the said facility, which could be implemented by the Banks."*

52. On 7th February, 2025, ld. Counsel for RBI had placed on record a circular dated 30th December, 2024, titled "***Introduction of beneficiary bank account name look-up facility for Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) Systems***". It was submitted on behalf of RBI that in view of the said service remitters using RTGS and NEFT mode of payments would be able to verify the name of the bank account to which the money is transferred before initiating the said transfer in order to prevent frauds. The RBI had also issued certain instructions to the banks in respect of the extension of the lookup facility to RTGS and NEFT. The Court was also informed that the said services would be fully implemented by 1st April, 2025.

53. In addition to the above, Mr. Susmit Pushkar, ld. Counsel appearing for NPCI was directed to file an affidavit in respect of the circular dated 30th December, 2024 addressing the measures to be taken by NPCI for achieving the deadline mentioned in the said circular. It was also directed that NPCI shall also address the process of verification of the name of the account holder before

initiating the transaction and the manner in which the same would be implemented.

54. On 7th February, 2025, Mr. Khan, ld. Counsel had brought to the attention of the Court a communication by NPCI dated 26th June, 2020 wherein certain steps have been taken to mitigate risks by misleading VPAs/UPI ids. One of the reference list of keywords includes brand names which are registered with the trademarks authority. Accordingly, the Court had directed NPCI and IBA to file affidavits in this regard.

55. Pursuant to the said directions, the concerned officials of NPCI being Mr. Ajay Shyam Pal, In-Charge Products and Mr. Nitesh S.K., Lead Product Development, were present in Court on 15th February, 2025. An affidavit dated 14th February, 2025 was also filed by NPCI in terms of the directions passed on 7th February, 2025. The Court perused the same and after considering the submission of Mr. Pushkar, ld. Counsel for NPCI, following directions were passed:

> *"22. It is noted that one of the important features of this affidavit is Annexure 1 which contains the indicative reference list of key words not to be allowed to individuals. The said list also contains names/marks of well known brands or companies which cannot be permitted to be registered as IDs of account holders without the permission of the said entity/brand holder. Further, the said list also includes various websites and well-known marks, organizational names, Government bodies, corporate designations which are not to be registered.*
>
> *23. It is submitted by ld. Counsel for NPCI that the said list is only an indicative list prepared by NPCI for the*

information of the banks and the same is not a definitive list. It is also submitted that the directions to the respective bank would have to be issued by the Court for refraining from registering a particular string of words. The NPCI does not have the power to implement the same.

24. Considering the said submissions, let the ld. Counsel for the NPCI take instructions as to whether upon a Court being satisfied that a brand or a mark has acquired a status which is well known and there ought to be an order directing that no individuals should be allowed to register bank accounts or UPI Ids or VPAs with the said brand names, an advisory can be issued by the NPCI to all banks in this regard, which would thereafter have to be implemented by the banks themselves."

56. Further to the above directions, on 5th April, 2025, Mr. Pushkar, ld. Counsel submitted that it would not be possible for the NPCI to issue an advisory to the banks in terms of an order of the Court directing that no individuals should be allowed to register bank accounts or UPI IDs or VPAs with certain brand names. It is further submitted that the creation of UPI IDs or the VPAs is the responsibility of the respective banks and not of NPCI, accordingly, it is up to the banks, who permit registration of the IDs, to ensure that there is no violation or use of key words which are impermissible. In view of this submission, the Court directed IBA to file an affidavit addressing the above, including the issue as to what measures can be taken by the IBA to ensure compliance by all banks of any order which may be passed by the Court directing that no individuals should be allowed to register bank accounts or UPI IDs or VPAs with the certain brand names.

57. The IBA had filed an affidavit dated 22nd May, 2025 pursuant to the above directions, in which the stand of the IBA and its members has been recorded. The same was considered by the Court on 27th May, 2025. Mr. Gautam, ld. Counsel for IBA, had clarified that the IBA is only a voluntary society of banks. Further, Mr. Srinivas Rao, Advisor to IBA was also present online through video conferencing and submitted that an advisory has been issued to all member banks of the IBA to strictly comply with the circulars and instructions issued by the Reserve Bank of India, including the ones considered by the Court, in the present proceedings.

Enforcement of Orders - Appointment of Grievance Officers by DNRs

58. Further to order dated 2nd June, 2022, wherein the Court had directed DoT and MeitY to file an affidavit disclosing their stand in respect of the privacy protect features provided by the DNRs, an affidavit dated 1st August, 2022 had been filed by MeitY. On 3rd August, 2022, the Court had considered the said affidavit as also the submissions made by Mr. Anil Kumar Pipal, Senior Scientist-F, MeitY. The relevant portion of the said order reads as under:

> *"18. Pursuant to the same, an affidavit dated 1st August, 2022 has been filed in CS(COMM) 135/2022. Some relevant submissions made by MeitY in the said affidavit are summarized as under:*
>
> - *NIXI cannot block domains in a blanket manner, as the same is against NIXI's policy framework, however it can block websites as per Court orders;*
> - *NIXI has market operations with DNRs located both within and outside India through Registrar Accreditation Agreements (RAA), whereby all DNR*

is mandated to share information of the domains with NIXI;

- *All domain name registries other than NIXI, if located in Indian territory, are bound to share WHOIS details of domains upon Court orders;*
- *In case of domain name registries outside India, the RAA does not obligate the registries to follow Indian law.*

[...]

21. On behalf of MeitY, Mr. Anil Kumar Pipal, Senior Scientist-F, has appeared and submits that though there are no regulations at present as to the manner in which it can be ensured that DNRs, especially those not in India, follow the orders of the Court or any Executive instructions. The same could be discussed internally and he would be willing to place a recommendation or a proposal before the Court on behalf of the Government."

59. In addition to the above, the Court was informed by Mr. Anil Kumar Jain, CEO, NIXI that it has agreements with 171 registrars in respect of registrations of *'.in'* and *'.bharat'* domain names. As per Clause 4.4.3. of the Registrar Accreditation Agreement of NIXI anonymous proxy registrations are barred and no privacy or proxy service can be provided. It was also submitted by Mr. Jain, that NIXI has implemented the General Data Protection Regulation, Regulation (EU) 2016/679 (hereinafter *"GDPR"*), and thus, NIXI has itself masked the details of the registrants. However, the said details would be provided in response to a Court order or request from a Law Enforcement Agency.

60. On 13th September, 2022, it was brought to the attention of the Court that the Plaintiffs are facing certain common issues in implementation of orders

passed by the Court against the DNRs. The Plaintiffs face difficulties in serving those DNRs who do not have their offices in India, as also in obtaining details of the Registrants of infringing domain names. In this regard, it was submitted by the Plaintiffs that the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter "*Intermediary Rules, 2021*") requires appointment of Grievance Officer, as part of the Grievance Redressal Mechanism, for handling complaints and implementation of orders passed by competent Courts. Considering the same, the Court had directed the DNRs to seek instructions and inform the Court –

(i) whether they have appointed the Grievance Officers in terms of the Intermediary Rules, 2021?

(ii) If yes, then provide the details of the same.

61. Accordingly, the matters were taken up on 14th September, 2022. The Court had heard submissions on behalf of various DNRs. It was submitted by Mr. Dayan Krishnan, ld. Sr. Counsel on behalf of the Newfold Group, consisting of six DNRs before the Court, that each of the said DNRs have appointed Grievance Officer. Further, the submission made *qua* the grievance redressal mechanism would be relevant and the same are extracted hereunder:

> *"23. In so far as the grievance redressal mechanism is concerned, Mr. Krishnan submits that the Newfold Group is in compliance with Rule 3(2)(a) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter "IT Rules 2021"), as whenever any complaint is made by any user or victim, the acknowledgment is issued to said user/victim, within 24 hours and the complaint is disposed of within 15 days from*

the date of its receipt. He further submits that if any order is issued by any Court of competent jurisdiction or any order, notice or direction is issued by a governmental or competent authority, the same would be complied with in terms of the IT Rules 2021. Similarly, if any order granting injunction or directions with respect to infringing domain names or other orders with respect to infringing domain names are passed by this Court or any Court of law, the Grievance Officer would facilitate giving effect to such orders and ensure that the same are complied with, upon receiving a communication at the email addresses set out above. Mr. Krishnan however, submits that considering the time differences and the fact that some coordination may be required for such compliance across different offices of the DNRs, reasonable time of 48 to 72 hours maybe afforded for the purposes of the said compliance.

24. These submissions on behalf of the Newfold Group are recorded and the Newfold Group shall be bound by the same, in all matters where infringing domain names are involved. If the said Grievance Officer is changed in the future, such change shall also be notified by prominently publishing it the websites of each of the entities of the Newfold Group."

62. Insofar as GoDaddy is concerned, it was submitted by Mr. Darpan Wadhwa, ld. Sr. Counsel, that they were unable to obtain instructions as to the status of appointment of a Grievance Officer under the Intermediary Rules, 2021. Further time was sought to verify the same. The Court, as last and final opportunity, permitted GoDaddy time till 20th September, 2022 for appointment of, or informing the Court about, the Grievance Officer as per the Intermediary Rules, 2021. Further, one week time was provided to all the DNRs providing

services in India for appointment of Grievance Officer, if not already done so, in compliance of the Intermediary Rules, 2021. In the event of failure to appoint the Grievance Officer by any DNR within the said period, the Court directed MeitY to take appropriate actions in accordance with law against the same. The relevant portion of the order dated 14th September, 2022 is extracted hereunder:

> *"36. If the said DNRs have not appointed Grievance Officers, one week's time shall be given to them for making the appointments in accordance with the IT Rules, 2021. If the said compliance is not made by DNRs, MeitY is free to proceed in accordance with law against such DNRs who are offering their domain name registration, hosting and related services in India, without complying with the local laws. A status report be put up by MeitY by the next date, on this aspect including the steps taken by MeitY pursuant to the directions contained above."*

63. Further, on 14th September, 2022, a status report was filed by MeitY informing the Court of the steps taken pursuant to the directions passed by this Court *vide* order dated 3rd August, 2022. The Court was informed that MeitY has prepared a questionnaire which has been shared with all the stakeholders and meetings have also been held with the same including ICANN, the Ministries, DNRs, Delhi Police etc. The DNRs were provided time till 30th September, 2022 to furnish their response to the said questionnaire. It was also directed that the meetings and deliberations shall continue and MeitY shall file its recommendations in respect of the issues highlighted by the Court *vide* order dated 3rd August, 2022.

64. Further to the above directions, the Court was informed on 11th October, 2022 on behalf of GoDaddy, and M/s. Hosting Concepts B.V. (hereinafter "*Hosting Concepts*") that both the said DNRs have appointed their Grievance Officers in terms of the Intermediary Rules, 2021. In view of the submissions made on behalf of the said DNRs, it was clarified that the paragraphs 23 and 24 of the order dated 14th September, 2022, extracted hereinabove, would apply *mutatis mutandis* to both GoDaddy and Hosting Concepts.

65. In respect of the directions passed on 14th September, 2022, *qua* appointment of Grievance Officers by the DNRs, a status report was filed by MeitY, wherein it was recorded as under:

> *"As of today, MeitY does not have powers to take action against non-compliant domain name registrars. On the order of the Hon'ble Court, action on blocking of website and email IDs would be taken. The power of such blocking is vested with DoT through ISPs."*

66. The said status report was considered by the Court on 10th February, 2023, and it was directed as under:

> *"6. It is noticed that there are two sets of DNRs which are operating in India.*
>
> - *The first sets of DNRs are those who offer various Global Top Level Domains (GTLDs) such as (.com), (.net) and (.org). Some such DNRs have agreed to appoint grievance officers and implement orders passed by Indian Courts/Authorities. However, a number of DNRs have either not responded to MEITY or have belatedly refused to comply with the orders passed by this Court.*

- *The second set of DNRs which operate in India are (.in) DNRs. In so far as (.in) DNRs are concerned, they are stated to have appointed Grievance Officers, as reflected in MEITY's report.*

7. In addition, ld. Counsel for the Plaintiffs in some of the matters have also informed the court that a number of DNRs have completely refused to comply with the blocking orders and other directions issued by this Court, in respect of infringing domain names.

8. In view of the aforementioned facts which have come to light through MEITY's status report, the submissions made before this Court from time to time and the e-mails which have been placed on record today, such as e-mails by Namecheap Inc, it is clear that stringent steps would be required to be taken, in order to curb the menace of illegal domain name registrations having well known marks and names of business houses. It is accordingly directed that MEITY/DoT/the appropriate authority shall take steps action in accordance with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 against DNRs who do not agree to comply with the said Rules or do not appoint grievance officers or implement orders of Indian Courts/Authorities.

[...]

10. It is directed that the concerned MEITY/DOT officials shall peruse the various orders which are passed in these proceedings prior to taking any action under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Steps in respect thereof, in terms of Rules be taken within four weeks. The

action so taken shall be placed on record by MEITY by means of a status report by the next date of hearing."

67. A status report dated 25th March, 2023, had been filed by MeitY pursuant to the above directions, which was considered on 27th March, 2023, addressing various issues including the following:

(a) **Action that can be taken by ICANN against DNRs which do not give effect to orders of the Court of competent jurisdiction:** It was informed by ICANN that under the Clause 5.5.2.1.4 of the Registrar Accreditation Agreement, ICANN may terminate the said agreement with the DNR in the event a competent Court determines that the DNR has failed to comply with an order in respect of domain names sponsored by the said DNR. It was clarified that termination of the agreement is only one of the many options available with ICANN under the agreement.

(b) **Implementation of Court orders:** MeitY has relied upon Section 69A of the Information Technology Act, 2000 (hereinafter "*the IT Act*") and Rules 3, 4, 6 and 10 of the Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009 (hereinafter " *Blocking Rules, 2009*"). It is stated that if there is repeated non-compliance of Court orders by any DNR, then the same can be construed as a violation of public order under Section 69A of the IT Act for blocking of the non-compliant DNR. However, a concern was also expressed to the effect that various Registrants could be inconvenienced if the website/URL of the non-compliant DNR is blocked.

68. In addition to the above, the Court was also informed on 27th March, 2023 of the orders passed by the ld. Single Judges in two suits *i.e.,* ***CS(Comm) 604/2022*** titled ***Star India Pvt. Ltd. vs. 7MOVIERULZ.TC & Ors****., and* ***CS(Comm) 567/2022*** titled ***Star India Pvt. Ltd. & Anr. vs. MHDTV.WORLD & Ors.,*** directing the DoT and MeitY to take action against five DNRs namely, NameCheap Inc., Dynadot LLC, Tucows Inc., Gransy s.r.o, and Sarek Oy, for non-compliance of Court orders. Further, on 26th May, 2023, the Court was apprised that insofar as NameCheap Inc., Dynadot LLC and Tucows Inc., are concerned, the same have moved appropriate applications stating that they are willing to comply with the orders of the Court and also appoint the Nodal Officers.

69. On 21st December, 2024, Mr. Pravin Anand, ld. Counsel, had placed a compilation before the Court and had highlighted services such as "*GlobalBlock*" and "*GlobalBlock+*", which as per the ld. Counsel are being provided by GoDaddy to provide protection to brands against unauthorised registration including for those which provide deceptively similar brands, homoglyph, variations and domain names with typographical errors of brands. The ld. Counsel had also placed reliance on the stand of Verisign Inc. (hereinafter "*Verisign*") in ***CS(Comm) 197/2024*** wherein Verisign, as a Registry Operator, has taken the position that the issues relating to blocking of domain names are purely in the domain of the DNR itself and not the Registry.

70. In view of the above submissions, the Court had directed GoDaddy to file an affidavit in respect of the services mentioned by Mr. Anand and on the difference between DNR and Domain Registry.

71. Pursuant to the said directions, an affidavit sworn by one Mr. John Massey had been filed by GoDaddy. The said affidavit was perused by the Court on 7th February, 2025 and Mr. Wadhwa, ld. Sr. Counsel had made his submissions in respect of the same. It was the submission of Mr. Wadhwa, ld. Sr. Counsel that the services "*GlobalBlock*" and "*GlobalBlock+*" are being provided by Brand Safety Alliance LLC, a subsidiary of the parent company of GoDaddy *i.e.,* Registry Services LLC (hereinafter "*Registry Services*"). The said entity - Brand Safety Alliance LLC, is stated to have agreements with various Registries in order to execute the said services. It is also submitted by Mr. Wadhwa, ld. Sr. Counsel that the blocking of domain names containing a particular word-string would be implementable only by a Registry and not by a DNR. Considering the above submissions, notice was issued to Registry Services and Verisign.

72. Further, the Court had also directed the DNRs to file their respective notes *qua* the directions which are being sought for injunction on specific word strings as also specific domain names including on the following aspects:

(i) What DNRs can do to implement orders being passed by Courts?

(ii) What are the steps DNRs cannot take which is in the scope of the Registry concerned?

73. Mr. Chander Lall, ld. Sr. Counsel had appeared on behalf of Verisign on 15th February, 2025 and requested time to file an affidavit in terms of the previous order. The Court after hearing the parties had directed as under:

> *"13. Pursuant to the order dated 7th February, 2025, notice was issued to the two Registries i.e., Registry Services LLC and Verisign, Inc., both the said parties have entered appearance before the Court. Mr. Chander Lall,*

ld. Sr. counsel appearing for m , Inc. submits that he would like to file an affidavit explaining the role of Verisign, Inc. and also the steps that can be undertaken by Verisign, Inc. if directions are given by the Court.

14. Specifically, both these parties i.e., Registry Services LLC and Verisign, Inc., shall file their affidavits in respect of the following aspects:

i. The domain name extensions that the said Registries manage and supervise;

ii. Whether in respect of the said domain name extensions, orders for suspension, locking, blocking and transfer of the domain names can be implemented by them in respect of existing infringing domain names;

iii. Whether the said Registries can also implement orders injuncting registration of infringing domain names in the future which contain the brands/trademarks as may be directed by the Court in the form of a TLD/word string.

15. In addition, National Internet Exchange of India (hereinafter "NIXI") shall also file an affidavit in respect of the above directions.

16. At the moment, the said two registries are not being impleaded in any suit of the present batch matters. Upon consideration of the affidavits which they file, the Court shall pass further orders in this regard."

74. Further to the above directions, on 5th April, 2025 ld. Sr. Counsels and ld. Counsels appearing for various DNRs and Registry Operators had placed on record their respective affidavits or notes and made submissions. Ms. Kruttika Vijay, ld. Counsel for Hosting Concepts BV had drawn attention of the Court

to the note dated 5th April, 2025, wherein examples of certain services which Hosting Concepts B.V. has signed onto as an accredited DNR, including the Trademark Clearinghouse (hereinafter "*TMCH*") have been mentioned. It is stated that TMCH is a global repository of validated and registered trademarks established by Internet Corporation for Assigned Names and Numbers (hereinafter "ICANN") to verify trademark data from multiple global regions and maintain a database with verified trademark records. The relevant paragraph of the said note is extracted hereunder:

> *"12. Some Registries provide services to brand owners through accredited DNRs to help protect the rights of brand owners on the Internet. Examples of services which Hosting Concepts has signed onto as an accredited DNR include:*
>
> *a. Trademark Clearinghouse (TCMH): TCMH is a global repository of validated and registered trademarks established by ICANN to (i) verify trademark data from multiple global regions; and (ii) maintain a database with the verified trademark records. Currently, ICANN has only authorized Deloitte to provide trademark verification services for TCMH. The advantage of TCMH include:*
>
> *i. Brand owners whose trademark rights are verified by TCMH are provided with a Signed Mark Data (SMD) file, which is recognized by several registries as proof of minimum eligibility requirements.*
>
> *ii. New gTLD registries utilizing TCMH are required to offer a sunrise period for registration of domain names to brand owners at least 30 days prior to*

public access.

iii. *On new gTLD registries utilizing TCMH, for a 90-day period after launch, registrants attempting to register a second-level domain name will receive a warning if the name matches an entry in the TCMH. If the registrant registers the name anyway, the rights owner will receive a notification from the Trademark Claims system.*

iv. *Rights holders with trademarks registered in the TCMH can opt in to receive additional notifications of exact matches to names they have registered in the TCMH."*

Privacy Protect Feature

75. In one of the suits, which was part of the batch matters, *i.e.,* ***CS(Comm) 176/2021*** titled ***Snapdeal Private Limited vs. GoDaddycom LLC & Ors.,*** the Court *vide* order dated 13th July, 2022 had observed as under:

> "*7. Ms. Shweta Sahu, ld. Counsel appearing for the Defendant Nos.1 to 4 submits that the Defendant No.1 - GoDaddy has an abuse policy, for example, which it has implemented which enables the trademark owners to fill up a form to seek suspension/locking of the domain name complained of. She submits that the same would then abide by the orders passed by the Court.*
>
> *8. This abuse policy may not be sufficient as the same still requires the IP owner to approach a court of law. The question that arises is as to whether the intervention of the Court would be required in every case involving registration of infringing domain names, particularly considering that they are registered in respect of lakhs and*

lakhs of domain names, especially for well-known trademarks. In fact DNRs offer alternate domain names on their own, without anyone seeking the same.

9. In the opinion of this Court, time has come for DNRs to create a mechanism by which any trademark owner who has an objection to the registration granted to any domain name, can approach the said DNR and seek cancellation/transfer of the said domain name. The same ought to be fairly considered through the mechanism which ought to be independent and impartial, for eg., through an Ombudsman. If the cancellation/suspension/transfer as sought is not agreed to through the said mechanism, then the IP owner can avail of its remedies in accordance with law.

10. Thus, there ought to be a mechanism where the abuse policy is not merely dealing with suspension/locking but should also be able to cancel/transfer the infringing domain names. Such an abuse policy should also be implemented by the DNRs through a specified set of officials based in India, to ensure that if in a case, the transfer/cancellation is not permitted under the abuse policy, the trademark owner would be able to avail of their remedies before the Courts in India, against such a decision of the DNR.

11. Ms. Sahu, ld. Counsel for Defendant Nos.1 to 4 submits that she would seek instructions in this regard. Accordingly, let an affidavit be filed as to whether an independent and impartial mechanism could be put in place by the Defendant Nos.1 to 4 to prevent the abuse of trade marks through registration of domain names, as also, to disable the privacy protect features and make available the details of the registering person in respect of domain names on the 'Whois' database. Let the said affidavit be

filed by 31st July, 2022."

76. Pursuant to the above, on 3rd August, 2022 the Court had heard the submissions on behalf of the Internet Corporation for Assigned Names and Numbers (hereinafter "*ICANN*"), and on behalf of certain DNRs. It was submitted by Mr. Darpan Wadhwa, ld. Senior Counsel on behalf of the DNRs that the DNRs provide the privacy protect features in compliance of their agreements with the Registry Operators and ICANN. The same is also necessary to meet the obligations under the GDPR. In response to the Court's query as to whether the said feature is mandatory or optional, the ld. Sr. Counsel submitted that the same is a bundled feature with no additional charges to the Registrant. It was also submitted that it is not the DNRs but the Registry Operators and ICANN which can decide how to proceed with privacy protect features. The Court had also perused the relevant agreements between ICANN and Registry Operators, as also between the Registry Operators and the DNRs. It was observed by the Court that the said agreements do not obligate DNRs to provide the privacy protect feature despite blatant infringement and fraudulent activities. Moreover, all Registry Operators and DNRs, under their respective agreements, *prima facie*, have to abide by and give effect to orders passed by competent courts, governmental authorities etc. However, the parties were directed to seek instructions to make more comprehensive submissions.

77. On 1st February, 2024, Mr. Darpan Wadhwa, ld. Senior Counsel appearing for GoDaddy made further submissions on the steps which may be taken in respect of non-compliant DNRs. He categorically, relied on the order dated 4th

December, 2023 of this Court in ***(CS (Comm) 303/2022)*** titled ***Burger King Corporation v. Swapnil Patil & Ors.*** to state that a similar order can be passed at the final stage and the examination in respect of all the identified domain names and the examination of additional domain names can be done by the Joint Registrar.

78. On 5th April, 2025 it was submitted in respect of the privacy issues by Ms. Kruttika Vijay, ld. Counsel for Hosting Concepts BV, that all accredited DNRs with ICANN are mandated to comply with the provisions of the General Data Protection Regulation passed by the European Parliament and the Council of the European Union. Further, Mr. Raj Shekhar Rao, ld. Senior Counsel appearing on behalf of ICANN submitted that insofar as the TMCH and privacy issues in the context of GDPR are concerned, ICANN has already addressed the same in its responses to the questionnaires provided by the Ministry of Electronics and Information Technology and the same are annexed with the written submissions filed by ICANN in ***CS(Comm) 228/2021*** titled ***Bajaj Finance Limited vs. Registrant of www.bajaj-finserve.org and others.***

V. STAND OF THE PARTIES

79. In the opinion of the Court, it would be apposite to first capture the position and stand adopted by various parties involved, to better appreciate the issues involved in the present batch of matters.

(A) ICANN – Internet Corporation on Assigned names and numbers

80. At the outset, Mr. Rajshekhar Rao, ld. Senior Counsel appearing on behalf of ICANN has submitted that ICANN does not submit to the jurisdiction of this Court. The submissions made by him are without prejudice to the said stand and

solely for the purpose of assisting this Court.

81. It is submitted by Mr. Rao, ld. Senior Counsel that the relationship of ICANN with the Registry Operators, and DNRs is governed by the respective agreements which exist between the said parties. He submits that ICANN merely receives data from the Registry Operators and DNRs. The ultimate control mostly exists with the DNRs and some powers are also vested with the Registry Operators. ICANN itself does not have any privity of contract with the Registrants and all policies of ICANN are implemented through the Registry Operators and DNRs.

82. He further submits that the manner in which ICANN functions is that it undertakes a complex process of evolving consensus amongst the members and various stakeholders including governments of several countries. Since, the entire functioning of ICANN is itself consensual in nature, it is submitted by the ld. Senior Counsel that ICANN cannot unilaterally submit any recommendations to the Court on a policy level. It is submitted that ICANN is not in a position to take any punitive or regulatory action against the Registry Operators and DNRs. However, ld. Senior Counsel submits that ICANN's position is clear that all DNRs have to comply with local laws and as the laws in each country continue to evolve, DNRs cannot escape the rigours of the law. Thus, any order passed by the Courts of competent jurisdiction would have to be implemented by the DNRs.

83. On a specific query from the Court as to whether privacy protect feature can be directed to be removed, ld. Senior Counsel highlights the quandary between the revealing of information on one hand and obligations under the

Digital Personal Data Protection Act, 2023 (hereinafter "*DPDP Act*") on the other hand. He submits that the owner of the data who registers the domain name should under the DPDP Act specifically permit revealing of the details, failing which, under the said Act, the DNR would not be able reveal without an order of a Court of competent jurisdiction.

84. On another query from the Court, as to whether DNRs hold domain names by proxies, it is submitted that some DNRs may be doing so but the question as to whether the same DNR or some group entity or associated entity is holding said registration would have to be tested on the facts of each case.

(B) <u>GoDaddy</u>

85. GoDaddy is a DNR having its headquarters in Tempe, Arizona, United States of America and incorporated in Delaware, United States of America. It provides domain name registration services for multiple generic Top-Level Domains (hereinafter "*gTLDs*") and several Country Code Top-Level Domains (hereinafter "*ccTLDs*"). GoDaddy complies with all the court orders that are passed. GoDaddy's stand is also that it is mandated due to the applicability of GDPR that all the details of the registrants have to be protected. GoDaddy claims that DNRs are mere intermediaries and are only required to act upon receiving actual knowledge by way of a order of the Court or a notification from the government. It complies with the necessary due diligence required under the IT Act and the Intermediary Rules, 2021. GoDaddy is not a significant social media intermediary. The mere fact that certain value added services are provided cannot deprive GoDaddy of the safe harbour protection.

86. The global block affidavit and global block services relied upon by the Plaintiffs are not provided by the GoDaddy but by its group company Brand Safety Alliance LLC. These services are provided at the registries' level and not at the DNR level. As per GoDaddy, it is only a registry which can block a particular words string as also particular words from being registered as domain names. This is beyond the capabilities of DNRs as per GoDaddy.

87. It was submitted by Mr. Darpan Wadhwa, ld. Senior Counsel on behalf of the DNRs that the DNRs provide the privacy protect features in compliance of their agreements with the Registry Operators and ICANN. The same is also necessary to meet the obligations under the GDPR. In response to the Court's query as to whether the said feature is mandatory or optional, the ld. Sr. Counsel submitted that the same is a bundled feature with no additional charges to the Registrant. It was also submitted that it is not the DNRs but the Registry Operators and ICANN which can decide how to proceed with privacy protect features.

88. It is submitted by ld. Senior Counsel that in the ***Snapdeal (supra)*** decision dated 18th April, 2022,[1] the injunction against a string used in a domain name has already been dealt with and the Court has held that the injunctions in such cases would have to be on specific domain name and not on a string. He further submits that there are more than 2500 DNRs that are operating and unless and until an order for dynamic injunction, similar to the order in ***UTV Software Communication Ltd. v. 1337X.To, 2019 SCC OnLine Del 8002*** is passed, a

[1] Judgement passed in I.A. 5407/2021 in CS(Comm) 176/2021.

DNR cannot be made to monitor the registration of domain names for infringement of trademarks. It is argued that offering of domain names cannot be held to be infringement of a trademark. He categorically, relied on the order dated 4th December, 2023 of this Court in ***(CS (Comm) 303/2022)*** titled ***Burger King Corporation v. Swapnil Patil & Ors.*** to state that a similar order can be passed at the final stage and the examination in respect of all the identified domain names and the examination of additional domain names can be done by the Joint Registrar. He also places importance on the decision of the Supreme Court of the United Kingdom in He also places importance on ***Cartier International AG and Others v. British Telecommunications Plc and Another, (2018) UKSC 28*** to argue that the cost of locking and suspending domain name, and continuing to retain control of the same, cannot be borne by the DNR but by the Intellectual Property owner who seeks such reliefs.

89. Ld. Senior Counsel also submits that the ISPs or DNRs cannot be expected to presumptively maintain a check in respect of well-known marks. By way of illustration, there could be a domain name 'Apple Stores' which could be offering counterfeit products and another 'Apple Store' could be offering the actual apple fruit online. It requires an adjudication or an examination to determine which domain name would be required to be blocked. It is submitted that the exercise under the Trademark Act, 1999 ought to be done by the Court and not by the DNR or the Plaintiff themselves. Moreover, trademark rights are territorial in nature and it has been seen in similar matters that there could be different registered proprietors in different jurisdictions for the same mark. Example of the decision of the US Court of Appeals in ***Toyota Motor Sales,***

***U.S.A., Inc. v. Tabari*[2],**. is cited in order to highlight the fact that even use of a brand like '*Lexus*' which is an invented mark is permissible under the nominative fair use doctrine.

90. According to Mr. Wadhwa, ld. Senior Counsel the only effective order that can be passed is against the Registry Operators and not against the DNRs, as was done against NIXI in the case of ***Burger King (supra)***. He further submits that under Section 79 of the Information Technology Act, 2000 (hereinafter "*IT Act*") the due diligence that is to be exercised by an Intermediary is only in respect of infringement of trademark which requires a Court order as held in ***Shreya Singhal v. Union of India, (2015) 5 SCC 1***.

91. It is highlighted by ld. Senior Counsel that GoDaddy operates within the scheme of the Registrar Accreditation Agreement, 2013 or other versions thereof, as required by ICANN, and under the said agreement:

(i) A format has to be followed for registration of domain names;

(ii) A verification system through either an email or a phone number is done;

(iii) Privacy issues are also to be given utmost importance, especially after the enactment of the GDPR which is the standard followed by ICANN;

(iv) The facilities of opt in or opt out is provided to the consumer;

(v) The movement has been towards protecting private data in order to prevent misuse and therefore by default, the privacy protect feature ought to be permitted. It is submitted by the ld. Senior Counsel that

[2] Toyota Motor Sales, U.S.A., Inc. v. Tabari, 610 F.3d 1171 (9th Cir. 2010).

disclosure of information ought to be the exception rather than the default rule.

92. On behalf of Goddady, it is also highlighted that there are similar cases which are dealt with by international jurisdictions. An example is ***Hermes International v. John Doe, 12-CV-1623(DLC) (SDNY April 30, 2012),*** is cited to show how the permanent injunctions are only against identified infringing domain names and additional infringing domain names have to be brought to the notice of the Court for the said injunction to be extended.

93. Mr. Wadhwa, ld. Senior Counsel has referred to Section 69A of the IT Act as also Rule 4 of the Intermediary Rules, 2021 to argue that both these provisions would not permit blocking of services of the Intermediary itself. These provisions at best permit blocking of the content which is violative of law. It is argued that even if the definition of the term '*public order*' under Section 69A of the IT Act is considered, the violation of a trademark or other IP rights cannot constitute a breach of public order. He thus submits that Section 69A of the IT Act itself would not be applicable in the present case and any blanket remedy in the form of blocking of the DNR to ensure compliance of Court orders would not be tenable. The blocking of services by a particular DNR being provided in India would in effect result in closure of the business of the said DNR, which would also have an impact on Registrants of various domain names to whom the said DNR may have provided services. Reliance is placed on the report of MeitY which mention that the blocking of Namecheap Inc, Diana LLC and Tucos Inc. adversely affected 2.5 lakh users in India.

94. Mr. Darpan Wadhwa, ld. Senior counsel has relied upon the written submissions filed by GoDaddy to argue that there are two types of DNRs, (1) who does not appear before the Indian Courts and are refusing to comply with the orders, (2) where there are DNRs who regularly appear before the Courts and there is merely delay in compliance. In the later case, the blocking of the business of the DNR ought not to be resorted to as the intention of the DNR is not to violate the orders of the Court but the delay could also be explainable. In the former case, he submits that the DNR itself ought not to be blocked as the same would be contrary to Section 69A of the IT Act, inasmuch as Section 69A of the IT Act merely contemplates removal or blocking of the information for access to the public but it does not contemplate the blocking of the intermediary as a whole.

95. In respect of the privacy and proxy services provided by the DNRs, ld. Senior Counsel has firstly relied upon the ICANN Registrar Accreditation Agreement, which is currently in force. Specifically, he refers to clause 3.14 and the certification of privacy and proxy registrations. The said clause 3.14 is extracted hereinbelow:

> "*3.14 Obligations Related to Proxy and Privacy Services. Registrar agrees to comply with any ICANN-adopted Specification or Policy that establishes a Proxy Accreditation Program. Registrar also agrees to reasonably cooperate with ICANN in the development of such program. Until such time as the Proxy Accreditation Program is established, Registrar agrees to comply with the Specification on Privacy and Proxy Registrations attached hereto*."

96. It is his submission that providing services through proxy servers and also providing privacy protect features is permissible under the ICANN Accreditation Agreement. In fact, it is his submission that after the enactment of the GDPR, the default position has to be protection of personal data. Reliance is placed upon Article 1, Article 4(5) and Article 25 of the GDPR and the same are extracted hereunder:

> ***"Article 1: Subject-matter and objectives**:*
>
> *1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*
> *2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.*
> *3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.*
>
> ***Article 4: Definitions**:*
>
> *4(5). 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*
>
> ***Article 25: Data protection by design and by default**:*
>
> *1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and*

purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*
3. *An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article."*

97. According to Mr. Wadhwa, ld. Senior Counsel the requirement for privacy protection is not merely an option, but in fact a mandate for all DNRs. He then relies upon the Temporary Specifications published by ICANN for gTLD Registration Data, which has in fact, implemented the GDPR and mandates that most data relating to the Registrants has to be redacted. Even in response to WHOIS query, only proxy/substitute email can be provided and nothing more.

GoDaddy, in fact, follows a policy called "*Request for Disclosure of Non-Public Registrant Information*" where anyone, who needs such information, can file either an IP complaint form, an abuse complaint form, or a domain name holder request form and the same would be duly processed as per the policy of GoDaddy.

98. It is also submitted, while placing reliance on Article 6 of GDPR, that the provisions of GDPR have to be strictly followed and that only in cases of 'legitimate interest' that override the interest of privacy would disclosure of information of a Registrant be permitted. On the basis of said provision, the ld. Senior Counsel submits that GoDaddy has adopted a mechanism wherein a specific IP complaint form and NPRD request form has been provided for raising complaints. It is submitted that as per the NPRD request form, one of the factors which would constitute 'legitimate interest' would be the ownership of any individual or entity over the intellectual property. If a party is able to show ownership over the intellectual property, upon a request being made *via* the NPRD form, GoDaddy would be required to investigate and respond to the said request withing a period of 30 days. It is argued that the such methods adopted by GoDaddy show that it is exercising its powers in a completely non-discriminatory and transparent manner.

99. Finally, reliance is placed upon the DPDP Act which also has laid down various obligations of entities processing personal data of individuals, such as GoDaddy. Further reference is also made to various definitions laid down in the DPDP Act including Sections 2(h), 2(j), 2(n), 2(t), 2(u) & 2(x). It is argued that in terms of the said provisions information of Registrants would be clearly

covered and thus would have to be protected from disclosure. The said sections are extracted hereinunder for ease of reference:

> *"2. In this Act, unless the context otherwise requires,—*
> *(h) "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;*
> *(i) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;*
> *(j) "Data Principal" means the individual to whom the personal data relates and where such individual is—*
> *(i) a child, includes the parents or lawful guardian of such a child;*
> *(ii) a person with disability, includes her lawful guardian, acting on her behalf;*
> *(k) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary;*
> *(l) "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10;*
> *(m) "digital office" means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;*
> *(n) "digital personal data" means personal data in digital form;*
>
> *xxx xxx xxx*
>
> *(t) "personal data" means any data about an individual who is identifiable by or in relation to such data;*
> *(u) "personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of*

access to personal data, that compromises the confidentiality, integrity or availability of personal data;
(v) "prescribed" means prescribed by rules made under this Act;
(w) "proceeding" means any action taken by the Board under the provisions of this Act;
(x) "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission,
dissemination or otherwise making available, restriction, erasure or destruction;

100. It is submitted by the ld. Senior Counsel that under Section 4 of the DPDP Act, data can be processed by a 'Data Principal' for a *lawful purpose* only if consent is given or for certain legitimate use. What constitutes the 'legitimate use', it is argued, can be seen from Section 7 of the DPDP Act. Specific reference is made to Sections 7(c), 7(d) & 7(e) of the DPDP Act. The same are extracted hereunder:

"**Section 4**

4. (1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—
(a) for which the Data Principal has given her consent; or
(b) for certain legitimate uses.
(2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

Section 7

7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:— [...]

(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(e) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;"

101. It is his submission that the consent from a data principal for disclosure under Section 6 of the DPDP Act has to be so clear and unequivocal that unless and until consent is obtained, the legitimate intent is to protect privacy at the highest.

(C) Hosting Concepts

102. Ms. Kruthika Vijay, ld. Counsel appearing for Hosting Concepts has submitted that the compliance with GDPR is mandatory for almost all DNRs,

especially, her client which is situated in Netherland. At the outset it is clarified by her that GDPR would only apply wherever the Registrant is a natural person and not a corporate or other business entity. Thus, in case of corporate or other non-natural business entity, the disclosure of data relating to the Registrant of the infringing domain name would not be covered by the GDPR.

103. She makes reference to Article 4 of GDPR to explain the process of *'pseudonymisation'*. Further, attention of the Court is also drawn to Article 5(1)(c) read with Article 25 of the GDPR as per which only minimum data which is required to be collected ought to be collected. This is also known as the concept of '*data minimisation*'. The DNRs, therefore, in compliance with the said provisions collect only the minimum required data which is necessary for processing the same.

104. She submits that the GDPR being an instrument which is applied by about 32 countries, various Courts and forums in different countries have interpreted it differently and thus, the implementation of the GDPR can prove to be challenging at times. Ms. Vijay, ld. Counsel describes GDPR as an amorphous legislation whereby the framework is changing continuously depending upon the interpretation which is adopted by the Courts. It is also submitted that the DNRs themselves need to be protected, failing which there would be huge implications for DNRs.

105. Reliance is also placed upon the *Temporary Specifications for gTLD (hereinafter "Temporary Specifications")* prescribed by ICANN and she submits that if there is any conflict between the Temporary Specification and the Registrar Accreditation Agreement, the former prevails. Thus, it is her

submission that the DNRs continuously struggle between ensuring compliance with the Registrar Accreditation Agreement and the Temporary Specification. It is further pointed out that in terms of the Temporary Specification, details of the Registrant have to be redacted and privacy is the default position. She further submits that the '*Registration Data Access Protocol Response Profile*' (hereinafter "*RDAP Response Profile*") published by ICANN, in fact, imposes further obligations upon the DNRs, such as, the manner in which the redaction has to be done. Specific reliance is placed upon Clauses 2.7 of the RDAP Response Profile, which deals with contacts and the redaction clause. It is argued by the ld. Counsel that in terms of the RDAP Response Profile protection of privacy is mandatory and there can be no compromise on the same.

106. Ms. Vijay, ld. Counsel has referred to a decision of the Court of Justice of the European Union[3] (hereinafter "*CJEU*") which concerned a request for preliminary ruling from the Supreme Court of Latvia in respect of interpretation of Article 7(f) of the *EU Directive 95/46/EC*[4] (similar to Article 6(f) of the GDPR).

107. Considering the above, ld. Counsel submits that insofar as Hosting Concepts is concerned, a model framework could be laid down for disclosure of the data of Registrants which may involve the following steps:-

[3] Case C-13/16 passed by the CJEU on 4th May, 2017

[4] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 7(f) reads as: "Member States shall provide that personal data may be processed only if: […] (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed , except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)."

(a) That the framework should require a request to be made in writing to the DNR, either through the Grievance Officer or through a web portal.

(b) The request should be credible and verifiable (such as a notarized affidavit with some basic conditions that are being satisfied therein).

(c) The same should be properly verified so that there is no fabrication or forgery.

(d) The Person requiring the information ought to indemnify the DNR for steps taken against an alleged infringing Registrant.

(e) The information should be capable of disclosure by the DNR in a Court or before any authority, if sought.

(f) In addition, she submits that other safeguards and exclusions ought to be that only verifiable rights can be considered by DNRs and not common law rights relating to pending applications.

(g) The standard of misuse or infringement alleged should be something which constitutes fraudulent or illegitimate use having a larger implication.

(h) If a particular website is being used for supporting for illegitimate purposes, upon the above facts having been satisfied, the privacy requirements can be suspended and disclosure of registrant details can be permitted. However, the same would also not result in either transfer or suspension of the domain name for which an appropriate Court would have to be approached. It is, therefore, her submissions that under national law proper frameworks can be evolved to deal with illegitimate and fraudulent websites.

108. Further, Hosting Concepts claims to be an intermediary and argues that it would not be liable for any third party content hosted on the website. As per the

affidavit dated it is stated that Hosting Concept shall comply with orders of the competent Court directing locking, suspension, cancellation or transfer of identified infringing domain names. It is also willing to disclose details of Registrants pursuant to directions being issued by the competent Courts.

109. According to Hosting Concept, the mechanism developed by the ld. Single Judge of this Court in ***UTV Software Communication (supra)*** ought to apply even to rogue websites in the present batch of matters. Insofar as preventive or automatic blocking of registrations of domain names is concerned, Hosting Concepts claims that the same is within the realm of the Registry Operators and not the DNRs. Finally, the position of Hosting Concepts on the blocking of future domain names is as under:

> *"5. Therefore, Hosting Concepts can comply (and has complied) with the orders of competent courts directing the locking, suspension, cancellation or transfer (at respective Plaintiff's costs) of the specifically identified domain names found to be identified as being illegally used by persons other than legitimate right holders, and will further comply with specific directions requesting disclosure of details of registrants of such domain names, where these details are redacted."*

110. It is also stated that Registry Operators are able to provide certain services/features such as Trademark Clearing House, Domain Protected Marks List and Adult Block, which would show the various tools/methods at the disposal of the Registry Operators to address the issues arising in the present matters. The nature of services that are provided under these features are as under:

*"a. **Trademark Clearinghouse (TCMH):** TCMH is a global repository of validated and registered trademarks established by ICANN to (i) verify trademark data from multiple global regions; and (ii) maintain a database with the verified trademark records. Currently, ICANN has only authorized Deloitte to provide trademark verification services for TCMH. The advantages of TCMH include:*

i. Brand owners whose trademark rights are verified by TCMH are provided with a Signed Mark Data (SMD) file, which is recognized by several registries as proof of minimum eligibility requirements.

ii. New gTLD registries utilizing TCMH are required to offer a sunrise period for registration of domain names to brand owners at least 30 days prior to public access.

iii. On new gTLD registries utilizing TCMH, for a 90-day period after launch, registrants attempting to register a second-level domain name will receive a warning if the name matches an entry in the TCMH. If the registrant registers the name anyway, the rights owner will receive a notification from the Trademark Claims system.

iv. Rights holders with trademarks registered in the TCMH can opt in to receive additional notifications of exact matches to names they have registered in the TCMH.

*b. **Domain Protected Marks List (DPML):** This is a service which is provided by the registry, Identity Digital for TLDs registered with it (e.g. army, info, legal). Broadly explained:*

i. DPML defensively blocks registrations of trademarked brands across the Identity Digital portfolio of domains. At time of purchase, all Identity Digital domain names matching the trademarked brand are reserved, allowing only the trademark

holder to register them going forward.
ii. To be eligible to access DPML, rights holders must hold an SMD file validated by TCMH.
iii. The DPML service is available only with respect to the trademarked brand with various gTLDs. For example, if the trademarked brand is "dabur", the DPML service can be used to defensively block registrations of dabur.army, dabur.info, dabur.legal etc.

c. ***AdultBlock:*** *This is a service which is provided by ICM Registry, which manages four different extensions: .xxx, adult, .porn and .sex.*
i. AdultBlock is available for any right holders (i) holding a TCMH SMD file, (ii) with a registered trademark in any jurisdiction, (iii) with an unregistered trademark (also called "common law trademark"), (iv) with a company or organization name, including "trading as", and (v) a celebrity wishing to protect their name.
ii. Domains that are already registered with ICM Registry at the moment the block is ordered are not included, but as soon as such domain is cancelled, it is added top the block."

111. In addition to the above, it is stated that ICANN also has a schedule of reserved name in terms of specification 5 of the RAA which is signed by all registries.

(D) <u>Newfold Digital Inc.</u>

112. One of the DNRs in the present suit with which certain infringing domain names have been registered is the Defendant No. 4 – Public Domain Registry Limited (hereinafter "*PDR*"), which is registered in the Republic of Seychelles

and stated to be a subsidiary of the Newfold Digital Inc. (hereinafter "*Newfold Group*").[5] At the outset, the stand of NewFold Group is similar to that of GoDaddy *i.e.,* that whenever orders are being passed by this Court they have been duly complied with by the Newfold Group. It is also stated that they are intermediaries under the IT Act.

113. On behalf of Newfold Group, Mr. Dayan Krishnan, ld. Senior Counsel had appeared and has firstly addressed the issue as to what orders the Court can pass in case a DNR does not comply with or adhere to the orders passed by the competent Courts in India in respect of either suspending, blocking or locking the infringing domain name. It is his submission that the business of the said DNR or the access to the DNR services cannot be blocked under Section 69A of the IT Act. The said provision is to be used only in case of exceptional circumstances as contained in the said section itself, *viz.* (i) sovereignty and integrity of India, (ii) defence of India, (iii) security of the State, (iv) friendly relations with foreigner States, (v) public order, and (iv) for preventing enticement to the commission of any cognizable offence relating to the said six circumstances. It is submitted by the ld. Senior Counsel that Section 69A of the IT Act cannot be used to enforce *inter se* rights of the trademark owners, which are commercial disputes in nature and thus, would be outside the purview of the said section.

[5] The submissions have been made on behalf of PDR and all other affiliates of Newfold Digital Inc., such as Endurance Digital Domain Technology LLP, BigRock Solutions Limited and Hostgator.com LLC, which have been impleaded as Defendants in other suits forming part of the present batch matters.

114. It is argued that the only term, which may need some consideration by this Court is '*Public Order*.' The said term, according to Mr. Krishnan, ld. Senior Counsel has already been decided by the Supreme Court in various judgments as public tranquility and safety. It is submitted that mere contravention of law would not affect public order, unless if affects the community or the public at large. In this regard, reliance is placed on the decision of the Supreme Court in ***Ram Manohar Lohia v. State of Bihar, AIR 1966 SC 740***. The submission is that mere non-compliance of Court orders by the DNRs does not amount to breach of public order, and a higher standard has to be adopted while invoking the provisions of Section 69A of the IT Act.

He further relies upon the following judgments: (1) ***Shreya Singhal v. Union of India, (2015) 5 SCC 1***; and (2) ***Google India Pvt. Ltd. v. Visaka Industries, (2020) 4 SCC 162.***

115. Mr. Krishnan, ld. Senior Counsel has also directed the attention of the Court to the Blocking Rules, 2009, specifically Rules 6, 7 & 8 to argue that the blocking of access to any information has to be in the manner as specified in the said Rules and, would thus require consideration from a Committee consisting of members not below the rank of Joint Secretary, as prescribed under Rule 7 of the Blocking Rules, 2009. Such a blocking of information is to be resorted to in extreme circumstances and not on a regular basis. He finally submits that certain situations may require legislative intervention and may be beyond the powers of the Court to block the business of the DNR. However, if the Committee under Rule 7 of the Blocking Rules, 2009 comes to a conclusion that non-compliance by the DNR could affect or infringe upon the sovereignty and integrity of India,

then it is up to the Government to take action. It is submitted that Rule 10 of the Blocking Rules, 2009 is not applicable to the present cases where there is violation of intellectual property rights and no blanket order for compliance ought to be passed.

116. He also relies upon the judgment in ***People's Union for Civi Liberties (PUCL) vs. Union of India, (1997) 1 SCC 301***, wherein the Supreme Court was dealing with Section 5(2) of the Telegraph Act which permits the Government to intercept messages, to argue that the said judgment also makes it considerably clear that such provisions must be construed narrowly and the same cannot be done unless the conditions mentioned under the said provision are satisfied. It is also submitted by the ld. Senior Counsel that orders may be granted giving liberty to the Plaintiffs for filing applications for impleadment of infringing defendants along with evidence.

117. Furthermore, as per the note dated 15th February, 2025 filed by the Newfold Group, in compliance of the Court's directions, the reliefs which can and cannot be implemented by the said DNR is as under:

Reliefs that can be implemented	Reliefs that cannot be implemented
Upon receipt of a court order, Newfold DNRs can: a. Suspend the domain name for the duration of its current registration.[2] Upon suspension, services connected to the domain name, such as email services are disabled and DNS. b. Lock the domain name (1) for the duration of its current registration to prevent transfer of the domain name;[3] or (2) until further order of the court. However, any direction to lock a domain name beyond its registration period would result in Newfold DNRs incurring costs, i.e., payment of fee to the relevant registry to prevent the domain name from falling into public domain. Intermediaries cannot be compelled to incur the costs of compliance to protect the rights of the plaintiffs.[4] c. Disclose registrant data of the domain name. d. Transfer the domain name to the plaintiff's account with the relevant Newfold DNR. **Note**: Subsequent orders can be passed by Joint Registrar (Judicial) of this Hon'ble Court on appropriate applications with affidavits filed by plaintiffs.[5] The above are in addition to the internal reporting channels made available by Newfold DNRs and ICANN, for example: https://publicdomainregistry.com/report-abuse-2/ https://www.bigrock.in/reports.php?action=report_spam	Newfold DNRs cannot: a. "Block", "block access", "take down" or "remove" a domain name.[6] Websites may be taken down by the web hosting service providers or blocked by internet service providers. b. Suspend a domain name permanently.[7] c. Block specific word strings or suspend all registered domain names which contain a specific word string.[8] *First*, it would result in circumvention of judicial scrutiny over the rights of third parties who may have a legitimate right to register such domain names. *Second*, domain names are not infringing on their own. *Third*, this would also require Newfold DNRs to actively monitor registrations of domain names for thousands of brand owners, which is far beyond their role as intermediaries;[9] it is a brand owner's responsibility to protect their own IP rights, not third parties such as Newfold DNRs.[10] *Fourth*, an order only against Newfold DNRs would cause serious prejudice, as the other 2400+ domain registrars can still offer such domain names. *Fifth*, Newfold DNRs do not own the domain names, they simply offers them for registration by contract with the registry. Registries, who own the domain names database and responsible for managing and operating top-level domains (TLDs), can block certain word strings from being offered for registration for the relevant TLD.[11]

118. Moreover, it is also stated that one of the terms of the registration of the domain name is that the Registrant ought not to use the services of the DNR in a way that infringes a patent, trademark, copyright or other IP rights. Further, it is also stated that ICANN and NIXI, both require compliance with local laws as also compliance with orders issued by the Court of competent jurisdiction. Lastly, it is stated that payment details of the Registrant with the DNR can be

provided in order to trace the person who has registered the domain name.

(E) <u>Verisign</u>

119. Verisign is a Registry Operator incorporated in Reston, Virginia, United States of America. At the outset, it is stated that Verisign does not have any offices or employees in India and does not carry on any business in India, hence, it is stated that Verisign does not submit to the jurisdiction of this Court. Verisign is stated to be the delegated Registry Operator for various TLDs namely '*.cc*', '*.com*', '*.name*' and '*.net*'. It is also the Registry Operator for certain internationalized domain names in various scripts:

a) .كوم
b) .点看
c) .קום
d) .कॉम
e) .コム
f) .닷컴
g) .ком
h) .คอม
i) .大拿
j) .नेट
k) .닷넷

120. The said TLDs are managed by Verisign in terms of the Registry Agreement with ICANN and the functions performed by Verisign are briefly set out below:

> *"6. Verisign is a Registry operator for certain Top-Level Domains ("TLDs") (as detailed below). As a Registry operator, it maintains the authoritative master directory of all second level domain name ("SLDs") in the TLD. The said master directory includes the following technical details relating to the registrations: (i) the SLDs (such as "verisign.com") for the TLD; (ii) the Internet Protocol ("IP") addresses (such as 192.42.177.30) of the name servers associated with the SLDs; (iii) the name of the Registrars of the SLDs; and (iv) the registration expiration dates of the SLDs."*

121. As is evident from the above, Verisign is one of the most important Registry Operator in the world as it controls the '*.com*' and '*.net*' domain name extensions, which are the most popular domain name extensions. More than 90% of the infringing domain names in the present commercial suits are '*.com*' registrations. Hence the stand of Verisign is crucial in deciding the issues that have arisen in these cases.

122. It is stated in the affidavit dated 2nd April, 2025 deposed by one Mr. Kirk Salzmann, authorised representative of Verisign, that Verisign does not provide any direct domain name registrations to end users. A Registrant who wishes to register a domain name with the TLDs operated by Verisign, has to get the same done through the DNR which has a Registry-Registrar Agreement with Verisign in respect of the said TLD. It is stated that most of the data relating to the Registrant lies with the DNR and not with Verisign. It also does not provide web hosting services. The nature of capabilities Verisign possesses are claimed to be limited. According to Verisign, the terms "locking", "blocking", "suspension" and "transfer" in respect of a domain name does not have a standard meaning or

definition across the relevant industry. Considering the same, it is stated that Verisign is capable of implementing status codes known as "*Extensible Provisioning Protocol*" (hereinafter "*EPP status codes*") to implement court orders of competent jurisdiction. The same are as under:

> *"a)* ***serverDeleteProhibited*** *- prevents a domain name registration from being deleted from the Registry. Deleting a domain name ends its registration and makes it available for others to register.*
>
> *b)* ***serverTransferProhibited*** *– prevents a domain name from being transferred from one Registrar to another. This does not prevent a domain from being transferred from one Registrant to another.*
>
> *c)* ***serverUpdateProhibited*** *– prevents certain aspects of the domain name (such as the name servers) from being updated.*
>
> *d)* ***serverRenewProhibited-*** *prevents a domain name registration from being explicitly renewed by the Registrar. However, it can still be auto-renewed.*
>
> *e)* ***serverHold*** *– prevents a domain name from resolving to a website. This means that the domain name is no longer active in the DNS and the corresponding website can no longer be accessed by typing the domain name in an internet browser. The website can, however, still be accessed via the IP address."*

123. In addition, it is submitted that if an order is received by Verisign for 'suspending' or 'blocking' of domain name, one of the steps that Verisign can take is to apply the '*severHold*' status code in respect of the said domain name,

in effect, therefore, even if the domain name is registered, the website would not accessible through the said domain name. Further, if the Court orders 'locking' of the domain name then it is stated that a combination of three status codes could be implemented *i.e., 'serverDeleteProhibited, 'serverTransferProhibited' and 'serverUpdateProhibited'*. However, it is stated that any order of the transfer of the domain name from one Registrant to another cannot be implemented by Verisign, as the same can only be done by the DNR. It is also necessary to note the fact that as per Verisign all the EPP status codes which are implementable by Verisign can also be implemented by the concerned DNRs.

124. On the question as to whether registration of infringing domain names in future can be prohibited, it is stated that Verisign does not have the technology to block particular word-strings. However, subject to approval of ICANN, certain character strings can be added to the "Reserved Names" list as per Clause 2.6 of the Registry Agreement, and any string added therein would not be registered by any Registrant. A perusal of the kind of word strings that can be blocked by Verisign is as under:

> *"26. The Registry Agreements entered into between Verisign and ICANN in respect of the .com, .net, and .name TLDs do not grant Verisign the authority to prevent the registration of any unregistered word strings. While the .com, .net., and .name Registry Agreements each include a list of character strings that Verisign is required to reserve and not make available for registration, no change to the lists can be made without explicit approval by ICANN (and amendments to the agreements). Furthermore, Verisign's registry systems for .com, and .net cannot "block" word strings from being registered as domain names. Such*

functionality is not part of Verisign's systems and could not be therefore implemented without changing the computer code and systems that operate those TLDs. The .com Registry Agreement dated 1 December 2024 entered into between Verisign and ICANN is attached herewith as Document 1. the .net Registry Agreement and the name Registry Agreement entered into between Verisign and ICANN are on similar lines as the .com Registry Agreement. The current standard form of the 'Base Registry Agreement' (as publicly available at https://www.icann.org/en/registry-agreements/base-agreement) ("Base RA") that is entered into between ICANN and some Registries, does entitle (under Clause 2.6) a 'Registry Operator' to reserve (i.e. withhold from registration) or block character strings within the concerned TLD. The IDNs operated by Verisign, listed above, are subject to the Base RA. A current standard form of the Base RA is attached herewith as Document 2.

27. Verisign has no ability to limit its actions on a geographic basis. Any action Verisign takes would apply globally. An order from a court of competent jurisdiction that prevents the registration of word strings (i.e. trademarks) as SLDs would effectively amount to a global injunction, restraining even genuine and bona fide users (including possibly prior users) and rights holders in other jurisdictions from using the concerned name strings as SLDs."

125. It is, however, clarified by Verisign that the action cannot be taken on a geographical basis and would have to be applied globally, which may negatively affect the rights of genuine and *bona fide* users in other jurisdictions.

(F) <u>Registry Services</u>

126. Registry Services is a Registry Operator having its registered office in

Wilmington, Delaware, United States of America. Registry Services operates and maintains administrative date of certain TLDs. As noted above, *vide* order dated 15th February, 2025 the Court had called upon Registry Services to disclose its stand on the following issues:

> *"i. The domain name extensions that the said Registries manage and supervise;*
>
> *ii. Whether in respect of the said domain name extensions, orders for suspension, locking, blocking and transfer of the domain names can be implemented by them in respect of existing infringing domain names;*
>
> *iii. Whether the said Registries can also implement orders injuncting registration of infringing domain names in the future which contain the brands/trademarks as may be directed by the Court in the form of a TLD/word string."*

127. Pursuant to the above directions, an affidavit dated 12th March, 2025 deposed by one Ms. Crystal Peterson, authorised representative of Registry Services, was filed in the batch matters. The said affidavit states that it provides services in respect of various TLDs, a large number of which are generic and ccTLDs. Registry Services has taken the position that it cannot implement any Court order for blocking, suspending or transfer of the domain names as it does not perform those functions as a Registry Operator. However, it can lock, hold, transfer, delete or reserve specific character stings. It does not provide any web-hosting services. It cannot implement the Court order related to management of domain names. It also cannot implement any Court order injuncting registering of infringing domain name in future.

(G) Stand of MeitY

128. During the course of these hearings it was found that several DNRs are not complying with the orders passed by the Court. This was resulting in continuous misuse of the infringing domain names, as also violation of the orders of the Court. After giving adequate opportunities to the DNRs, in some cases, the Court took a strict stand and directed that those DNRs who are not implementing the Court orders ought not to be permitted to provide their services in India. Some such orders which have been passed by this Court are extracted below:

Order dated 9th November, 2022:[6]

> *"10. Mr. Kurup, ld. CGSC appearing for MeitY and DoT, submits that as and when the Plaintiffs have notified the departments about various infringing websites, which are involved in illegal streaming of the Plaintiffs' contents, proper blocking orders have been issued. If the Court has passed suspension and disclosure orders, the DNRs ought to have taken action in accordance with law. He however submits that through VPN networks, these DNRs may still be accessible, thus allowing streaming/hosting/etc. of infringing content to continue.*
>
> *11. In the backdrop of the above discussion, insofar as the above listed DNRs, which are not giving effect to the orders of this Court, i.e., NameCheap Inc./Defendant No.13, Dynadot, LLC/Defendant No.14, Tucows Inc./Defendant No.16, Gransy s.r.o./Defendant No.17, and Sarek Oy/Defendant No.18, since DoT and MeitY are present before this Court,* ***they are directed to immediately take action within one week against these DNRs for non-***

[6] Star India Pvt. Ltd. & Anr. v. MHDTV World & Ors., CS(COMM) 567/2022.

compliance of the orders passed by this Court. The authorities shall also look into the question as to whether these DNRs ought to be permitted to continue to offer their goods and services in India, if they are not giving effect to orders of Indian Courts and not complying with the applicable laws under the Information Technology Act, 2000, and the 2021 Rules.*"*

Order dated 21st March, 2023:[7]

"4. The relevant directions passed by the Court in CS(COMM) 567/2022 on 9th November, 2022, are set out below:

> *"11. In the backdrop of the above discussion, insofar as the above listed DNRs, which are not giving effect to the orders of this Court, i.e., NameCheap Inc./Defendant No.13, Dynadot, LLC/Defendant No.14, Tucows Inc./Defendant No.16, Gransy s.r.o./Defendant No.17, and Sarek Oy/Defendant No.18, since DoT and MeitY are present before this Court, they are directed to immediately take action within one week against these DNRs for non-compliance of the orders passed by this Court. The authorities shall also look into the question as to whether these DNRs ought to be permitted to continue to offer their goods and services in India, if they are not giving effect to orders of Indian Courts and not complying with the applicable laws under the Information Technology Act, 2000, and the 2021 Rules."*

5. ***In view of the above, the defendants no.38 and 39 are directed to take appropriate action against the defendant no.23, Gandi SAS and defendant no.25, NameSilo, LLC,***

[7] Star India Private Limited v. 7movierulz.tc & Ors., CS(COMM) 604/2022.

for non-compliance of the order dated 2nd September, 2022 and file status report within four weeks from today.

Order dated 10th February, 2023:[8]

"7. In addition, ld. Counsel for the Plaintiffs in some of the matters have also informed the court that a number of DNRs have completely refused to comply with the blocking orders and other directions issued by this Court, in respect of infringing domain names.

8. In view of the aforementioned facts which have come to light through MEITY's status report, the submissions made before this Court from time to time and the e-mails which have been placed on record today, such as e-mails by Namecheap Inc, ***it is clear that stringent steps would be required to be taken, in order to curb the menace of illegal domain name registrations having well known marks and names of business houses. It is accordingly directed that MEITY/DoT/the appropriate authority shall take steps action in accordance with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 against DNRs who do not agree to comply with the said Rules or do not appoint grievance officers or implement orders of Indian Courts/Authorities.***

9. Ld. Counsel for the Plaintiffs are free to communicate with the official from MEITY Mr. Pradip Verma, who shall act as the nodal officer for this purpose to coordinate with DoT and any other authorities, at the e-mail address pradip.verma@meity.in and submit their respective lists of DNRs who are stated to be not complying with the orders passed by this Court and not appointing the grievance officers.

[8] Dabur India Limited vs. Ashok Kumar & Ors., CS(COMM) 135/2022

> *10. It is directed that the concerned MEITY/DOT officials shall peruse the various orders which are passed in these proceedings prior to taking any action under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Steps in respect thereof, in terms of Rules be taken within four weeks. The action so taken shall be placed on record by MEITY by means of a status report by the next date of hearing."*

129. These orders were to be implemented through MeitY/DoT. Upon their services being blocked from being offered in India, some of the non-compliant DNRs moved appropriate applications before the Court and undertook to implement the relevant Court orders, which then led to lifting of the directions to block the said DNRs.

130. Further, in the written submission dated 26th May, 2023 filed on behalf of MeitY reliance is placed on the decision of this Court in ***Snapdeal Pvt. Ltd. v. Godaddy.com LLC, 2022 SCC OnLine Del 1092***, wherein the Court has dealt with various issues *qua* DNRs and domain names *vis-à-vis* trademark infringement. It is argued on behalf of MeitY that in terms of the said judgement DNRs are intermediaries under the IT Act and the DNRs would be liable to forego the 'safe harbour' protection under Section 79 of the IT Act, where the domain names sold by the DNRs infringes the registered trademark of a third party.

131. In respect of enforcement of orders against non-compliant DNRs is concerned, the stand of MeitY is that the course of action taken by this Court in ***Star India Pvt. Ltd. & Anr. v. MHDTV World & Ors., CS(COMM) 567/2022*** *vide* order dated 9th November, 2022 when enforced in conjunction with Rule 10

of the Blocking Rules, 2009, is the only effective mechanism for ensuring that non-compliant DNRs duly comply with the Court orders. Moreover, it is stated in the status report dated 25th March, 2023 that where a DNR repeatedly does not comply with the directions of the Court, the same would be construed as a violation of public order under Section 69A of the IT Act.

132. In addition, Mr. Harish Vaidyanathan Shankar, ld. CGSC relies upon his written submissions to canvass the position that the judgment in ***Shreya Singhal (supra)*** makes it clear that in case there is contempt of Court or any other factors as contemplated in the Article 19(2) of the Constitution of India, the power of blocking would exist. He submits that the Article 19(1) of the Constitution of India is meant to protect legitimate businesses and not those businesses who are complicit in fraudulent activities being carried out. Thus, ***Shreya Singhal (supra)*** is a decision where the Court can rely upon to block a DNR from offering services in India.

133. Considering the above position as also the implications and significance of the issues involved in these batch matters, the Court was of the opinion that the Government *i.e.,* MeitY should also take a stand in this matter as to how to curb the proliferation of infringing domain names which were having a large scale impact on consumers and the general public. Further, pursuant to the directions passed by this Court in the batch matters, MEITY undertook a stakeholders consultation with different entities including the DoT, ICANN, Delhi Police etc. It is stated that MeitY had also issued a questionnaire to various entities including ICANN, DoT, NPCI, NIXI, various DNRs, CERT-IN, Cyber Law & e-Security Division of MeitY, and Delhi Police. A meeting was also held

by MEITY with all these stakeholders. Some of the feedbacks received are as under:

(i) <u>Response received from ICANN</u>

134. ICANN's position in respect of implementation of Court orders is captured below:

> "*4. That Internet Governance Division of MeitY followed up with the Internet Corporation for Assigned Names and Numbers (hereinafter referred to as 'ICANN') on the issues involving domain name infringement and non-compliance of DNRs in a related matter. !CANN, in its response placed at Annexure I, has· submitted as follows. That Section 5.5.2.1.4 of the RAA (Registrar Accredited Agreement) states that !CANN may terminate a registrar's RAA where a court of competent jurisdiction determines that the registrar has failed to comply with the terms of an order issued by a court of competent jurisdiction relating to the use of domain names sponsored by the registrar. If evidence is received, I CANN Contractual Compliance would follow its established process and take enforcement action as permitted by the RAA. The RAA provides various means of redress for consideration; termination of the RAA is not the only option provided."*

135. In respect of the privacy protect feature and proxy services provided by the DNRs, it was stated by ICANN that providing privacy services to Registrants is optional and at the discretion of the DNRs. The relevant portion of its response reads as under:

> *"**Additional Comments***
>
> *While the MeitY specifically requested (i.e., requested orally during the meeting on 27th December 2022)*

ICANN's input on court-identified issues 1 and 7, ICANN also provides the below comments concerning certain of the other draft recommendations set forth by the MeitY.

With respect to court-identified issue no. 2 (concerning privacy and proxy registration services), ICANN does not obligate registrars to offer privacy or proxy services to registrants. Providing such services is optional, at the discretion of the registrars. However, registrars that do choose to offer privacy or proxy services (themselves or via a registrar's affiliated entities) must comply with the RAA's Specification on Privacy and Proxy Registrations. This Specification requires privacy and proxy service providers to publish their processes to report abuse of a domain name and infringement of trademarks or other rights of third parties, and to include privacy and proxy customer contact information in the registrar's data escrow deposits. The ICANN community has also, via the multistakeholder Policy Development Process, developed recommendations for the creation of a privacy and proxy service provider accreditation program. ICANN's implementation of this program is currently paused pending further implementation efforts on related Consensus Policy recommendations concerning gTLD registration data."

136. ICANN has implemented the Uniform Domain Name Dispute Resolution Policy (hereinafter "*ICANN UDRP*") and Uniform Rights Suspension System (hereinafter "*ICANN URS*") which can be availed of by the trademark owners in the event of infringing domain names. It would be in compliance with GDPR to request access to registrant's data through the DNRs or ROs. The access to the Registrant's details is merely restricted but not barred. One of the legitimate interest which is an exception and permits disclosure of data is for the purposes

of consumer protection, investigation of cyber crime, DNR abuse and intellectual property protection.

137. MEITY's status report dated 25th March, 2023, also states that the Government of India's representative to the Government Advisory Committee of ICANN had highlighted the issue of domain name abuse in the meeting held between 11th to 16th March, 2023. Considering the growing abuse of DNRs, the importance of 'WHOIS Accuracy' was highlighted as a method for curtailing the said abuse. The Government continues to have its deliberations with ICANN in this regard. The said status report also highlights that India is a member of WIPO based UDRP procedure, which also provides online despite resolution mechanism.

(ii) Response received from HIOX LLC

138. HIOX Softwares Pvt. Ltd. (hereinafter "*HIOX*") is a DNR situated in India having its registered office in Coimbatore, Tamil Nadu. In its response to the questionnaire circulated by MeitY it was stated that HIOX has adopted mobile OTP verification and Aadhar verification process for providing domain name registrations. It was also stated that foreign and Indian DNRs ought to be mandated to follow the KYC process. Further, it is stated that privacy policy ought to be made a paid service and the WHOIS details can be shared with the authorised party upon an email being received from a person having a 'legitimate interest' or through a Court order. Even if privacy services are availed of parties who have a 'legitimate interest' cannot be deprived of data. All DNRs or Registry Operators which operate in India have to mandatorily follow the Indian law. The details of payments received such as credit card details, etc., can be

made available only to authorised LEAs, however, the payment gateways do not seek consent of the party for providing details to LEAs.

(iii) Response received from CERT-IN

139. The main issue raised by CERT-IN is that the identity of persons registering domain names is masked and most of the details are fictitious and not traceable. Thus, it is stated that a process needs to be put in place for obtaining the WHOIS details of the domain name.

(iv) Response received from Cyber Law and e-Security Division, MeitY

140. It is stated that blocking of domain names cannot be done under Section 69A of the IT Act unless it involves national security or public order issues.

(v) Response received from NIXI

141. NIXI has introduced e-KYC policies for ensuring accuracy of WHOIS details of the Registrant as per the government records. It has issued general instructions to DNR to avoid registration of the domain names which resemble well-known trademark. It is stated that on receiving a complaint from a well-known trademark owner regarding infringement, arbitration process under "*.IN Dispute Resolution Policy*" has to be initiated. NIXI upon receiving a Court order or an order from an authorised agencies blocks a disputed domain on a permanent basis. It is stated that NIXI's equipped to become a data repository provided due acceptance is received from the competent authority.

(vi) Response received from NPCI

142. In respect of the question whether NPCI can share the details of the accused with the LEAs and/or aggrieved persons in the event of an unlawful activity, it is stated that NPCI only shares transactional information with the

LEAs under the CrPC. NPCI would not be in a position to assist LEAs with the identity of a cyber-criminal, however, the relevant banks would be available able to do so.

(H) <u>Stand of MHA</u>

143. Pursuant to the orders passed by this Court on 24th November, 2023 and 1st February, 2024, the MHA had convened a meeting on 1st April, 2024 headed by the Chief Executive Officer, I4C with the different LEAs to understand the issues faced by them in respect co-ordination and receiving information from intermediaries. Another meeting was also convened on 10th April, 2024 headed by the Joint Secretary, Cyber & Information Security, MHA. In the said meetings various problems were highlighted and it was agreed that there is a need for a common online portal to integrate LEAs, banks and financial intermediaries to take action against financial cyber frauds. It would be relevant to mention few of the issues highlighted in the said meetings:

(i) Need for centralised system to obtain information from foreign domain name registrars and registries.

(ii) IT Intermediaries should collect necessary KYC and payment details to help identify persons violating the law online.

(iii) Privacy protection features used in WHOIS databases are being abused by criminals and information necessary for investigation, upon request, should be made available to LEAs.

(iv) Details from domain registrars, hosting agencies and mail service providers should be readily available for investigation.

(v) Actual IP address should be accessible where domain proxy services are

used. Additionally, details of other domains owned by the same person should be provided.

(vi) WHOIS database entries should include administrative details, payment information, IP addresses, SSL certificate provider agency details, and KYC details.

144. As per MHA various steps have been taken to implement the directions of this Court *qua* improving the co-ordination between various agencies to prevent cybercrime, specially relating to financial fraud. A portal *i.e.,* 'National Cybercrime Reporting Portal' for reporting online cybercrime and lodging complaints has also been made operational by I4C. Further, more than 38.87 lakhs complaints were reported on the said portal which is now the centralised portal where complaints for reporting of cybercrimes. In addition, I4C has also constituted seven Joint Cyber Coordinate Teams have been constituted for dealing with cybercrime cases. Lakhs of SIM cards and thousands of mobile devices have been blocked to prevent cybercrime.

(I) Stand of the Delhi Police

145. The Delhi Police has created the IFSO to look into the misuse of well-known marks in misleading domain names, websites and URLs. Pursuant to the various orders passed by this Court investigation was conducted in the respective suits against the alleged accused persons using the infringing domain names for committing financial frauds. In the course of the said investigations, several issues and challenges have arisen for the Cyber Cell of Delhi Police as also the IFSO. The same have been highlighted by the Cyber Cell, Delhi Police in its

written submissions dated 26th September, 2023.

146. It is stated that whenever any domain name or website is used in the commission of crime, the details are collected from the DNR as also the web hosting company. The mode in which the payment is made to the DNR or the web hosting services is also collected. The details are obtained from the bank accounts and the mobile numbers which are available. It is also stated that 'Voice over Internet Protocol' applications are presently not being traced.

147. The challenges faced by Delhi Police are that most intermediaries from abroad do not furnish details of the Registrants of the infringing domain names in view of privacy policy and insist on warrants or assistance through the Mutual Legal Assistance Treaty (hereinafter "*MLAT*") which delays the obtaining of information considerably. In contrast, domestic intermediaries provide better assistance however, foreign intermediaries having server in foreign countries tend to deny information arbitrarily.

148. One of the biggest road blocks in safeguarding the money in cases of online financial fraud is that the responses from banks is not satisfactory. There are no anti-fraud measures put in place by banks and e-wallets. The banks and financial institutions are not open post working hours and on weekends, though, they provide services to their own customers even during the said break. Banks ought to have a single window system for redressing cyber frauds and providing information to LEAs.

149. As per Delhi Police, bank accounts are being opened by bank officials without proper verification of the account holder in online bank accounts there is no physical verification. Intermediaries do not disclose how the payment is

received for registration of the domain name and the sub-domain.

150. Details of intermediaries providing cloud services, web hosting services and mode of payment is also not furnished. IP address captured while creating the domain or sub domain is not furnished. The mobile numbers which are given by domain name registrants are either wrong or do not exist, thus, the OTP verification at the time of registration of the domain name ought to be necessitated upon.

151. In addition to banks and financial institutions, the Cyber Cell has also highlighted the issues with social media intermediaries such as Google. It is stated that agencies such as Google ought to be directed not to provide promotional services such as adword, bookings, search engine optimisation to infringing domains and websites. Further, it is stated that Google does not respond to data disclosure requests and the standard automatic reply received is as under:

> *"All requests for the disclosure of data must be accompanies by appropriate legal process… all communications be sent from an official government issued email address."*

(J) Submissions on behalf of the Plaintiffs in the batch matters

152. Since, the present suit has been heard along with a batch of matters raising common issues, where similar grounds have been raised by the Plaintiffs, for the sake of brevity it would be apposite to consider together all the submissions raised by the Plaintiffs in the batch of matters.

153. Mr. Anirudh Bhakru, ld. Counsel had appeared for the Plaintiff in the lead matter *i.e.,* ***CS(Comm.) 135/2022*** titled ***Dabur India Ltd. v. Ashok Kumar*** and made submissions. He has firstly highlighted two orders passed by this Court dated 2nd June, 2022 and 3rd August, 2022 wherein the issues were crystalized and the Court has clearly observed that the present system of registering domain name is unsatisfactory. It is submitted that though the status of the DNRs is that of intermediaries, the intermediaries are also benefiting by offering a full range of domain names consisting of the Plaintiff's mark. If such a range of domain names is permitted to be offered, as held in the same would constitute trademark use and, therefore, the DNRs are not merely intermediaries but they do owe responsibility as well.

154. He has relied upon the decision of the ld. Single Judge of this Court in - ***Snapdeal Pvt. Ltd. v. Godaddy.com LLC, 2022 SCC OnLine Del 1092***, which dealt with the trademark infringement and registration of domain names consisting of the mark '*Snapdeal*'. In the context of this case, the ld. Single Judge observed that use of the domain names by DNRs for the purpose of registration and offering of the same especially for profit, would constitute 'use' under Section 2(2)(b) of the Trade Marks Act, 1999 (hereinafter "*the TM Act*"). The said decision it is also held that the allegation of infringement by use in the course of trade of the alleged infringing domain name can also be raised against the DNRs. It is further submitted that insofar as the said decision is concerned, the Court held DNRs responsible if the DNR is using the domain name registration as a model for generating profits by providing alternative domain names. If that is so, the judgment holds clearly that the DNR would lose the status of

intermediary. Insofar *quia timet* actions are concerned, the Court merely held that an order in *futuro* restraining any domain name cannot be passed and the Court would have to examine the matter *qua* the concerned domain name.

155. It is submitted that Section 79(2)(c) of the IT Act read with Rule 3(1)(b)(iv) of the Intermediary Rules, 2021 mandates that an intermediary is required to undertake due diligence in order to ensure that Intellectual Property rights are not infringed. Thus, failure of the DNRs to undertake due diligence as mandated would make them liable to forego the safe harbour protection.

156. It is the submission of ld. Counsel that the Court has to first look at the nature of the mark, determine if it is an inventive mark and grant the highest level of the protection *i.e.* permanent injunction against use and registration of the said mark as a prefix. In the case of generic marks, the Court could modify the injunctions or could direct the trade mark owner to approach the Court and obtain an order. The order of injunction, that can be granted, ought to be granted depending upon the nature of the trade mark, for which protection has been sought.

157. Ld. Counsel also relies upon the decision in ***Google LLC v. DRS Logistics (P) Ltd., (2023) 4 HCC (Del) 515*** to argue that in the case of ad-words, where trademarks have been monetized to be used as an ad-word, the Division Bench of this Court has already held that the intermediary would be liable even for contributory infringement. The intermediary, therefore, has to make adequate effort to stop violation and infringement by them, failing which DNRs could be made responsible even for substantial amounts of damages.

158. The last aspect, which has been highlighted is in respect of *de facto* privacy being provided to all Registrants. The said feature, which has been provided by most DNRs, especially GoDaddy, is resulting in masking the actual culprits and the domain names, which are worth more, are blocked. The lack of KYC while registering domain names is the root cause of all these fraudulent activities. In fact, DNRs, who are earning substantial sums of money are not found forwarding any solution. It is his submission that they also exhibit an abhorrence to comply with the orders passed by the Court and technicalities are cited to justify non-compliance. He also submits that even when the information is provided by the DNR, the same is so unsatisfactory that no effective action can be taken against the registrant of the domain name. Ld. Counsel submits that KYC ought to be introduced in order to safeguard the interest of third stakeholder in these matters *i.e.,* the consumer/victim, who may loose money and as has been seen in all these suits, the said victims/consumers hardly ever get back their money. The lacuna is at different levels, banking levels as also at the DNR levels, since they are unregulated. There is hardly any diligence being exercised by the DNRs.

159. Ld. Counsel finally submits that even one week of fraudulent websites being permitted to operate could cause enormous damage to the public. Thus, it is not only the Plaintiff's interest that is to be kept in mind but also the public interest.

160. Mr. Sidharth Chopra, ld. Counsel appearing for several Plaintiffs including HT Media Ltd., Bajaj Finance Ltd., Hindustan Unilever Ltd., and Fashnear Technologies Pvt. Ltd., has made the following submissions:

(a) at the outset submitted that the orders by which services of DNRs were

blocked through ISP in India pursuant to order of this Court in ***Star India Pvt. Ltd. & Anr. v. MHDTV World & Ors., CS(COMM) 567/2022***, was a measure which was required to be taken in the context of complete non-compliance by DNRs of the orders passed by the Court. He submits that when the Court orders were communicated to DNRs, such as Namecheap Inc., Hostinger, GoDaddy.com etc., the stand taken by them was that unless and until an order from a Court in United States of America is received, they would not be bound by the same. The ld. Counsel has taken the Court through various emails from Namecheap Inc. including emails dated 22nd August, 2022, 6th October, 2022, 22nd February, 2023 and 13th March, 2023.

(b) It is submitted that after Namecheap Inc. took the position of non-compliance of this Court's orders, the respective Plaintiff approached the Court and thereafter the orders for blocking of the services of the DNRs, including Namecheap Inc. was passed. Pursuant to the same, *vide* email dated 13th March, 2023 the concerned Plaintiff was informed that millions of customers of Namecheap Inc. have been affected due to the blocking order and that Namecheap Inc. was willing to provide the information sought. Ld. Counsel submits that the said email reveals the manner in which unless and until coercive measures were directed by the Court, there was no compliance by the DNRs. Some DNRs, including Namecheap Inc. even took the position that this Court's order is not a government order and no affidavit would be filed before the Court by Namecheap Inc., since Namecheap Inc. is not required to comply with a foreign Court's order. It

was also stated that it is only a voluntary supply of information relating to the registrant's details of illegal domain name. Reference is made to email dated 30th January 2023, 15th February, 2023, and 22nd February, 2023 to argue that in fact, Namecheap Inc went to the extent that it ought to be deleted from the array of parties as it cannot be compelled to comply with the orders passed by the Court.

(c) A similar situation arose in case of Hostinger, which also moved an application before the Court that the Grievance Officer is being appointed only for *'.in'* domain names and that thousands of customers were facing access issues to their websites and domain names due to the blocking orders. Similar position was also taken in an application filed by Dynadot LLC as well, which claims that millions of customers are affected by the blocking order.

(d) It is his submission, therefore, that the DNRs, who do not comply with the orders passed by the Court, a strict action ought to be taken against them. Reliance is also placed upon the decision of the ld. Division Bench in ***Department Of Electronics and Information Technology v. Star India Pvt. Ltd., 2016 SCC OnLine Del 4160*** wherein the Court has clearly directed that the strict action ought to be taken to curb violations and the government and its instrumentalities have a duty to assist in the enforcement of orders passed by the Court.

(e) Mr. Chopra, ld. Counsel also submitted that in none of these matters, the DNRs challenged the rights of the Plaintiff in the marks or brands. The only question is as to how the orders are to be enforced. It is his submission that

stringent measures ought to be permitted as without such measures the rule of law itself is under threat.

(f) He relies upon the Section 69 and Section 69A of the IT Act to argue that if the emails such as those written by Namecheap Inc. are ignored, it poses threat to the sovereignty of this country, which need not only be territorial sovereignty, compliance of orders of Court is an integral part of the sovereignty.

(g) Further, it is his submission that the cascading effect of non-compliance is also necessary to be borne in mind as there is no deterrence against such non-compliance. The DNRs though having no competing interest also benefit from making available domain names, which violate trademark rights. In such cases, the interest of the public, which has been duped, is of paramount nature. In fact, Civil Courts ought to have the powers, bearing in mind judgement in ***Department Of Electronics and Information Technology v. Star India Pvt. Ltd., 2016 SCC OnLine Del 4160*** that a preliminary enquiry ought to be directed by the police authority so that the details of the persons, who have registered the domain names and for freezing orders to be passed against the bank accounts, where the amounts are kept. Such orders would be required to be implemented through police as, failing which, the fraud is continued to be perpetuated.

(h) Targeted remedies as done in case of dynamics and dynamic plus injunctions with sufficient safeguards would protect the interest of IP owners as also strike at the violations. It is his submission that finally a judicial oversight would be required for directing enquiry by the police

under Section 161 of the Code of Criminal Procedure, 1973. After which upon obtaining information, the IP owner can go to the Court seeking appropriate remedy.

161. Mr. Abhishek Singh, ld. Counsel appearing in three suits of Amul, Bajaj Finance Ltd. and ITC Ltd. has made the following submissions:

(a) submits that there is no identifiable data whenever such domain name registrations are being permitted by masking of the details. In fact, he relies upon the provisions of the DPDP Act and submits that under Section 2(t) of the said Act, the personal data of any individual ought to be an identifiable data and Section 3 of the same also makes it adequately clear that so long the services are being provided in India, the Act would apply to the data, which is outside the territory of India.

(b) Ld. Counsel further submits that in a case like AMUL, 90 Defendants have already been impleaded and there are more which need to be impleaded. He emphasises that only generation of an email is sufficient and the said email itself becomes the identity of the Registrant, without any further details, which is leading to the proliferation of such infringing domain names. Finally, Rule 3 of Intermediary Rules, 2021 is also relied upon to argue that reasonable efforts have to be made by the intermediary to ensure that there is no infringement of IP rights such as trademarks under Rules 3(b)(iv). He emphasises that reasonable efforts are not even been made by the DNRs to avoid infringement as the finding of infringement has already been rendered against them in the decisions, which are being relied upon.

162. In addition to the above, written submissions have been filed by the Plaintiffs in each of the suits in the batch matters, wherein the following broad submissions have been made:

(a) The DNRs, which generate a substantive portion of their revenues from India, ought to be directed to comply with the orders passed by the Courts. Under the IT Act, there are several obligations upon the DNRs, which they need to comply with and non-compliance of the orders passed by the Court ought to be vested DNRs with consequences such as foregoing the safe harbour protection. Any non-compliance of Court orders ought to be construed as violation of public order and sovereignty under Section 67A of the IT Act. The internal sovereignty could be effected in case of non-compliance by the DNRs. Under the IT Act, designated officer can punish with imprisonment if there is non-compliance. Non-compliant DNRs also pose threat to compliant DNRs as they would get monetary benefits if domain names are transferred from one DNR to the other by the Registrant. Internet governance would be substantially effected if the DNRs are permitted to violate orders by the Court. Hence stringent measures are required.

(b) Notice ought to be also issued to the ISPs, banks to disclose details of whatever data is available with them in respect of bank accounts, mobile numbers, payment gateway information etc. Matching of the beneficiary name should be mandatory and not merely matching of the account number. During investigation, the bank accounts have been debited and, therefore, there should be immediate bank account freezing upon commencement of

investigation.

(c) Dedicated email ought to be provided for accessing data. DNRs ought to be directed to transfer the infringing domain names. Privacy protected features should not be permitted to be abused. Expedited blocking for well-known marks should be sought for domain names registration. Any non-compliant DNRs not to be permitted to undertake any future transactions from India.

(d) When the criminal complaints are initiated, arrests are made and victims of these frauds were found in several countries of the world like USA, UK, Canada, South Africa, and Netherland. Sometime infringing domain names also perform services of domain name servers operating from foreign countries. Multiple suffixes *i.e.,* domain name extensions, which are made available, made the process of tracing domain name fraud impossible and till some major illegality is detected by then it is too late. The process under MLAT or the Hague Convention[9] is quite time consuming.

(e) DNRs are not entitled to safe harbour protection as they are not merely acting as intermediary but are also consciously promoting registration of infringing domain names by providing multiple services including alternate domain name registration wherein the trade mark is also used as alternate extensions etc. The DNRs have created algorithm to facilitate their own businesses and are not ignorant of the alternate domain names, which are being presented for registration. They also fail to undertake due diligence as required under law.

[9] Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters.

(f) The DNRs are not merely intermediaries as they offer various services such as 'Global Block', 'Global Block Plus', which are paid services. They also have technology blocking specific words, words strings etc. The role of the Registry Operator is limited. It is the DNR, who can block the domain name.

VI. ANALYSIS AND FINDINGS

163. Heard ld. Counsels for the parties who have entered appearance in the present batch of matters.

164. It is pertinent to note that none of the contesting Defendants against whom allegations of use of infringing domain names have been raised, have appeared before this Court or participated in the proceedings which have been continuing since 2022.

Prevention of financial frauds

165. The commercial suits involving fraudulent domain names, initially seemed to be one-off cases. However, after the constitution of the IP Division of the Delhi High Court, a clear pattern started emerging wherein there were a large number of such suits were being filed by brand owners which then warranted a comprehensive and consolidated mechanism to deal with these situations. It was realised that in some of these commercial suits the financial fraud which had taken place was running into crores of rupees. Cyber cells of various police agencies were intimated, complaints were registered. In fact arrests of a few persons was also made in some cases. FIRs were also registered in a large number of cases and the proceedings in those cases are going on. However, in order to consider as to whether there can be some coordinated and structured solution to this problem of financial frauds using reputed trade marks and brand names,

notice was issued to the RBI and to various other banks where the accounts were opened by these unscrupulous and infringing entities/ individuals.

166. The individual banks came forward with their KYC data revealing the identities of the persons who had opened the bank accounts. Such persons had given their mobile numbers and through the said mobile number some individuals were traced. However, in most cases, the Registrants and the ultimate beneficiaries are still unknown or untraceable.

167. One of the major causes of amounts being transferred in favour of such infringers was also because the innocent persons who were making payments did not realise that they were not making payments to the actual brand owners or business owners such as Colgate or to Dabur but in fact to some unconnected individuals. In order to plug this clear loophole that existed in NEFT and RTGS transactions, notice was also issued to the NPCI. After several orders been passed from time to time, the RBI introduced the ***'Beneficiary Bank Account Name Lookup'*** facility for RTGS and NEFT system, on 30th December, 2024. In terms of the said facility, all banks were directed to adhere to the following instructions:

"(CO.DPSS.RPPD.No.S987/04.03.001/2024-25 dated December 30, 2024)

Introduction of beneficiary bank account name look-up facility for Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) Systems

1. To ensure that remitters using RTGS and NEFT systems can verify the name of the bank account to which money is being transferred before initiating the transfer and thereby avoid mistakes and prevent frauds, a solution for fetching

the beneficiary's name is being implemented. Based on the account number and IFSC of the beneficiary entered by the remitter, the facility will fetch the beneficiary's account name from the bank's Core Banking Solution (CBS).

2. This facility shall be made available to remitters through Internet banking and Mobile banking. The facility shall also be available to remitters visiting branches for making transactions.

3. To ensure uniform experience for customers, the banks shall adhere to the instructions given below:

i. Provision to verify beneficiary bank account name shall be provided in Internet banking and Mobile banking facilities at the time of registering a beneficiary and at the time of one-time fund transfer where the beneficiary may not be registered.

ii. Provision to re-verify a registered beneficiary at any time shall also be provided.

iii. Beneficiary account name provided by the beneficiary bank shall be displayed to the remitter.

iv. In case the beneficiary name cannot be displayed for any reason, the remitter can proceed with the fund transfer, at her discretion.

v. Specific alert messages as provided in the technical document, issued earlier by NPCI, shall be displayed to the remitter.

4. Both remitting and beneficiary banks shall preserve detailed logs of all queries made, responses received and all other activities as part of beneficiary bank account name lookup facility.

5. NPCI shall not store any data relating to this facility. In case of a dispute, the remitting bank and the beneficiary bank shall resolve the dispute based on the unique lookup reference number and the corresponding logs.

6. While providing the facility, banks shall ensure to comply with legal provisions related to data privacy, if any.

7. Beneficiary account name lookup facility shall be made available to customers without any charge.
8. All banks who are direct members or sub members of RTGS and NEFT are advised to offer this facility no later than April 1, 2025."

168. Banks were also directed through the IBA and the Central Economic Intelligence Bureau (hereinafter "*CEIB*") to share information with LEAs. A direction was given on 15th April, 2024 for finalisation of a Standard of Procedure (hereinafter "*the SOP*") for sharing of information by banks with LEAs. The said SOP was finalised and was issued on 31st May, 2024.

169. With the issuance of the RBI circular and the SOP issued by the Department of Revenue CEIB to all banks, the issue relating to the name of the recipient becoming visible to the payer has been resolved. Even the sharing of information from banks to LEAs has also been resolved. The IBA in its affidavit dated 22nd May, 2025, has clearly stated as under:

"2.5. That subsequently, RBI vide its mail dated 10/0112024 informed that a High-Level Meeting on prevention of cybercrimes was held by RBI with a team of Senior Officials from Ministry of Home Affairs (MHA) including I4C and DGPs of some States. The LEAs were of the view that there was a need for Banks to expedite:-
(i) Response to the complaints lodged on National Cybercrime Reporting Portal (NCRP);
(ii) Response to the complaints lodged over weekend/ long holidays as the crime rate spikes during such time period;
(iii) Timely sharing of information sought by LEAs etc.
Copy of Email dated 10.01.2024 received from RBI is annexed herewith and marked as ***Annexure A-2.***

2.6. That to examine the issues referred by RBI, IBA had constituted a Sub Group of 11 Banks to discuss on the above points and to place the deliberations before the Standing Committee and Managing Committee of IBA. The Sub Group deliberated on the subject and made suggestions for further streamlining the process and a draft SOP was designed and shared with CEIB on 15/05/2024. The same is annexed herewith and marked as ***Annexure*** *A-3 .*

2.7. ***That in compliance of the Order dated 15.04.2024 passed by this Hon'ble Court, the Central Economic Intelligence Bureau (CEIB) prepared the revised and updated SOP dated 31.05.2024 and forwarded the same to all concerned Authorities as mentioned in the said OM dated 31.05.2024 while forwarding a copy of the same to Indian Banks' Association also****.*

2.8. ***That the Indian Banks' Association has forwarded the aforementioned revised SOP dated 31.05.2024 prepared and circulated by the Central Economic Intelligence Bureau to all the Member Banks vide mail dated 03.06.2024 for doing the needful****. Copy of the mail dated 03.06.2024 addressed by Indian Banks' Association to all the Member Banks along with OM dated 31.05.2024 issued by the CEIB is annexed herewith and marked as* ***Annexure A-4***

2.9. That with regard to the Circular dated 26.06.2020 issued by NPCI to all PSP's and Third-Party Application Provides - UPI, IBA has nothing more to add. Copy of the Circular dated 26.06.2020 issued by NPCI is annexed herewith and marked as ***Annexure*** *A-5.*

2.10. ***That as regard the Circular dated 30.12.2024 issued by the RBI to all Banks participating in RTGS and NEFT Systems, it is submitted that the said instructions dated***

30.12.2024 issued by the RBI are binding on all the Participating Banks in view of Section 10 (2) read with Section 18 of Payment Settlement Systems Act, 2007 and IBA has nothing more to add*. Copy of the Circular dated 30.12.2024 issued by the RBI to all Banks participating in RTGS and NEFT Systems is annexed herewith and marked as* ***Annexure*** *A-6."*

170. In terms of the affidavit of the IBA extracted above, all banks are required to adhere to the SOP and to the RBI's circular on beneficiary name lookup facility. Insofar as digital payments through UPI and other payment apps are concerned, the recipient's name becomes visible when such a payment is made. However, the infringing websites were taking advantage of the non-visibility of the recipient's name while making payments through RTGS and NEFT, which now is a loophole that has been fully plugged with the introduction of the RBI's circular dated 30th December, 2024.

171. However, at this stage, the Court is required to adjudicate the various issues arising in relation to the use of infringing domain names and in effective protection of the trademarks of the Plaintiffs. In view of the detailed hearings conducted and the submissions of the parties, the following issues have been identified to be addressed in the present proceedings:

(i) What are the obligations and liabilities of a DNR in respect of an alleged infringing domain name registered with the said DNR? Whether the said obligations are sufficient for protecting the intellectual property rights of third parties?

(ii) What measures may be directed by the Court to be implemented by the

DNRs to safeguard the trademarks of the Plaintiff?

(iii) What measures may be directed by the Court against DNRs who refuse to comply with the Court orders?

(iv) Directions

(v) Relief to be granted in the Applications seeking interim relief.

ISSUE I: WHAT ARE THE OBLIGATIONS AND LIABILITIES OF A DNR IN RESPECT OF AN ALLEGED INFRINGING DOMAIN NAME REGISTERED WITH THE SAID DNR? AND WHETHER THE SAME ARE SUFFICIENT FOR PROTECTING THE INTELLECTUAL RIGHTS OF THIRD PARTIES?

Domain Name System

172. At the outset it is expedient to understand the manner in which the domain name registration system works and the various players or entities that are involved in this system.

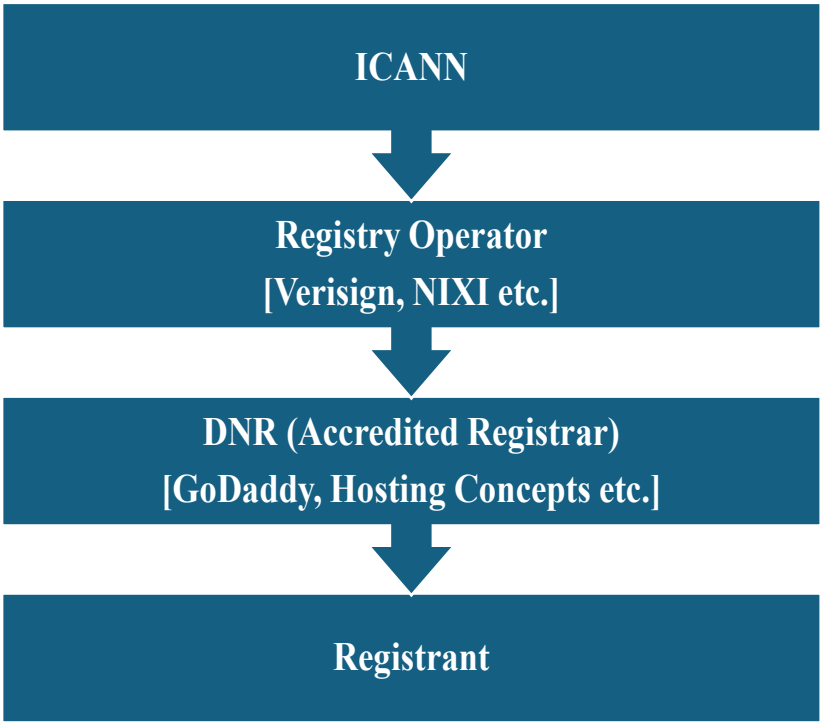
173. It is common knowledge that to communicate between different computers/devices across the internet, each computer/device is assigned a unique numerical identifier which is referred to as the Internet Protocol address or IP address. A domain name represents the IP address or other resource, in the form of a string of letters instead of the numerical identifier. This makes it easier for the user of internet to access websites etc., by searching for the familiar string of letters such as "www.google.com", instead of using the corresponding numerical address (*i.e.,* 172.217.0.78).

174. The domain name system, thus, acts as an address book for the internet. This address book is coordinated across the world by ICANN which is a not-for-

profit organisation that, *inter alia*, prescribes the policies that govern the domain name system. ICANN prescribes the technology that has to be used, the standards that are to be maintained and how the various protocols would function. In ICANN's own words its role is described as under:

> "***What Does ICANN Do?***
> *To reach another person on the Internet you have to type an address into your computer -- a name or a number. That address must be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination, we wouldn't have one global Internet.*
>
> *In more technical terms, the Internet Corporation for Assigned Names and Numbers (ICANN) helps coordinate the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS). The IANA functions include: (1) the coordination of the assignment of technical protocol parameters including the management of the address and routing parameter area (ARPA) top-level domain; (2) the administration of certain responsibilities associated with Internet DNS root zone management such as generic (gTLD) and country code (ccTLD) Top-Level Domains; (3) the allocation of Internet numbering resources; and (4) other services."*

175. There are several stakeholders involved in the functioning of the domain name system and registration of domain names - each entity having a fixed role within the system. The said system is illustrated hereunder:



176. Thus, a Registrant who wishes to register a domain name would avail the services of a DNR, which is accredited with ICANN to offer domain name registration services in respect of specific global Top-level domains viz., *gTLDs* such as '.com,' '.org,' '.net,' '.info' etc. The relationship between the Registrar and ICANN is governed by the '*Registrar Accreditation Agreement*'. The said DNR would also have to enter into an agreement with the respective Registry Operator known as the '*Registry-Registrar Agreement'* to get access to a particular TLD. Moreover, the Registry Operator would also have to enter into an agreement known as the '*Registry Agreement*' with ICANN to obtain the rights to maintain particular TLDs. At the stage of registration, the registrant enters into an agreement known as the "*Domain Name Registration Agreement*" with the DNR. In effect there are four agreements which bear significance on the

issues under consideration:

(a) Registry Agreement entered between ICANN and Registry Operator;

(b) Registrar Accreditation Agreement between ICANN and DNR;

(c) Registry-Registrar Agreement between Registry Operator and DNR; and

(d) Domain Name Registration Agreement between DNR and Registrant.

177. Thus, in order to identify the obligations and liabilities of the parties in respect of an infringing domain name, it would be necessary to consider each of the above said agreements.

Role of Registry Operators: ICANN - Registry Agreement

178. As mentioned above, each Registry Operator such as NIXI, Verisign, Registry Services, etc., would have to enter into a Registry Agreement with ICANN. In terms of the said agreement, a Registry Operator shall be capable of giving accreditation to DNRs. The Registry Operator has to comply with the policies of ICANN including its bye-laws. It has to show that it has secured the funds for operating the registry. The Registry Operator has to operate through ICANN accredited DNRs except in some cases where the registry itself is offering domain name registration services. All domain name registrations for a particular TLD have to be registered through the accredited DNR which in turn has to have an agreement with the Registry Operator. The code of conduct of such registries are prescribed by ICANN. Registries are expected to provide monthly reports as per the agreement with ICANN. It also stipulates as to how the Registry Operators have to operate WHOIS services. The format of the same is provided in Specification No. 4 of the Registry Agreement. Specification No.

5 to the Registry Agreement also provides the schedule of reserved names that are known as ASCII labels. Such labels include expression such as 'www', 'WHOIS', 'DNS' etc., and names belonging to countries and territories, names of internationally reputed organisations such as International Olympic Committee, International Red Cross, the Red Crescent Movement, Intergovernmental Organisations etc.

179. **Clause 2.8 of the Registry Agreement lays down one of the covenants of the Registry Operator in respect of *'protection of legal rights of third parties'*. As per the said clause, the Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement, governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD.** In addition, the Registry Operator is also required to comply with the provisions of Specification No. 7 to the Registry Agreement which mandates adherence and implementation of all the Rights Protection Mechanism in respect of Trademark Clearinghouse. The ICANN maintains a **Trademark Clearing House Database** (hereinafter "***TMCH Database***") which is a central database providing information to Registry Operators and DNRs, as also to the DNS to support protection of trademark rights. This TMCH Database stores information relating to trademarks which are registered on the database. Whenever any Registrant seeks to register a domain name matching with a trademark record existing on the database, a notice is given to the said registrant in respect of the possible infringement of an existing trademark. In addition, parallelly, a notification is also given to the trademark holder that such a domain name which is matching to the trademark has been

registered. This database acts as a caution to Registrants of any attempt to register a conflicting domain name, which could conflict with its trademark rights in order to enable the trademark owner to decide to take action, if so required.

Role of DNRs: Registrar-Accreditation Agreement

180. The role of DNRs is governed not only by the Registrar Accreditation Agreement entered into between ICANN and DNRs, but also as per the obligations under the Registry-Registrar Agreement and the Domain Name Registration Agreement executed with a Registry Operator and a Registrant, respectively. The said agreements with the Registry Operator and the Registrant, respectively, would differ for different parties. However, the same would have to comply with the provisions of the Registrar Accreditation Agreement. Thus, in order to completely appreciate the DNR's role in respect of protecting the rights of third parties from trademark violation as also in complying with Court orders, the Court has considered and examined the Registrar Accreditation Agreement.

181. The various obligations of the DNRs under the Registrar Accreditation Agreement are set out hereunder:

(a) Submitting the 'Registered Name Holder Data' to the Registry Operator, including the domain name, IP addresses of the nameservers, identity of the Registrar, and expiration date of the domain name, as also any other data mandated by the Registry Operator.

(b) Providing free public query-based access to data on registered names, including the following:

(i) domain name;

(ii) creation and expiration of the registration;

(iii) name and postal address of the Registrant;

(iv) name, postal address, e-mail address, voice telephone number of the technical contact for the domain name;

(v) The name, postal address, e-mail address, voice telephone number of the administrative contact for the domain name.

(c) However, subsequent to enactment of GDPR, the disclosure of Personal Data by the DNR would be subject to the Consensus Policy adopted by ICANN as also the Registration Data Directory Services (hereinafter "*RDDS*") Specifications.

(d) The data in respect of the Registrant and the registered domain name is to be made available to ICANN for inspection and copying.

(e) DNRs shall abide by applicable laws and governmental regulations.

(f) DNRs shall not register or renew any domain name which is included in a list of names reserved from registration as maintained by the concerned Registry Operator for the gTLD.

(g) DNRs shall conduct reasonable and commercially practicable verification, at the time of registration, of contact information provided by the Registrant, as also conduct re-verification of such information.

(h) Upon being notified by any person as to the inaccuracy of any contact information in respect of a registered domain name, the DNR shall take reasonable steps to investigate and rectify the same.

(i) DNRs shall receive complaints of abuse of registered domain names including DNS abuse and illegal activity. Upon receiving actionable

evidence of the said abuse, the DNR shall promptly take appropriate mitigation actions that are reasonably necessary to stop or disrupt the said abuse.

(j) ICANN may terminate the Registrar Accreditation Agreement where a Court of competent jurisdiction has held:

(i) the DNR to have permitted an 'Illegal Activity'[10], with actual knowledge or through gross negligence in the Registrant providing inaccurate registration data to the DNR;

(ii) the DNR has failed to comply with an order of the Court;

(k) ICANN may also terminate the Registrar Accreditation Agreement if it finds based on its review of the findings of arbitral tribunals, to have been engaged in use of domain names identical or confusingly similar to a trademark or service mark of a third party in which the Registrant has no rights or legitimate interest, which trademarks have been registered and are being used in bad faith.

182. In addition to the above obligations, the DNRs are also required to comply with various specifications issued by ICANN, including the WHOIS Accuracy Specification. The said specification requires validating and verification of the information provided by the Registrant in respect of the registered domain name. The DNR is required to validate within 15 days of the registration the following

[10] The term 'Illegal Activity' has been defined under Clause 1.13 of the Registrar Accreditation Agreement (2013) as: "Illegal Activity" means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.

information:

(a) Presence of data for all fields in a proper format of the respective country;

(b) All email addresses, telephone numbers and postal addresses are in proper format;

(c) Postal address fields are consistent across fields *i.e.,* street exists in city, city exists in state/province, city matches postal code.

183. The DNR is also required to verify the contact information of the Registrant, including the email and the telephone number through a tool-based authentication method providing a unique code, in the following terms:

> *"i. the email address of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response* ***through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by Registrar****, or*
>
> *ii. the telephone number of the Registered Name Holder (and, if different, the Account Holder) by either* ***(A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code*** *that must be returned in a manner designated by Registrar, or (B)* ***calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the Registered Name Holder via web, email or postal mail****.*
>
> ***In either case, if Registrar does not receive an affirmative response from the Registered Name Holder, Registrar shall either verify the applicable contact information***

manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration."

184. Where the Registrant has wilfully provided inaccurate or unreliable contact details, and the Registrant wilfully fails to respond within 15 days of the inquiries by the DNR as to the accuracy of information, the DNR shall either terminate or suspend the domain name, or place the registration on '*clientHold*' and '*clientTransferProhibited*', until the DNR has validated the information.

NIXI - Registrar Accreditation Agreement

185. At this stage it would also be necessary to note that NIXI has its own Registrar Accreditation Agreement in respect of '.in' ccTLDs. All major DNRs have agreements with NIXI for registration of the domain names with '.in' extensions (hereinafter "*the NIXI Agreement*"). Certain obligations of the DNRs registering '.in' domain names differ from the obligations under the corresponding agreement with ICANN. The same are captured in brief hereunder:

(a) DNRs shall refrain from directly or indirectly cooperating with any Registrant who violates or instigates violation of rules, regulations and laws prevailing in India. The DNR shall be responsible for informing NIXI in case of any violation by the Registrant;

(b) DNRs shall submit data of the Registrant to NIXI, including the domain name, IP address of the nameservers, and other data mentioned in clause

4.3 of the (hereinafter "*the NIXI Agreement*").

(c) DNRs shall provide public access to data on registered domain names in the following terms:

> ***"4.3. Public Access to Data on Registered Names.*** *During the Term of this Accreditation Agreement:*
>
> *4.3.1. At its own expense, Registrar shall provide an interface or link to the ccTLD WHOIS. The information to be made available shall include:*
> *4.3.1.1. The registered name;*
> *4.3.1.2. The names of the primary name server and secondary Name server(s) for the Registered Name;*
> *4.3.1.3. The identity of the Registrar (which may be provided through Registrar's Website);*
> *4.3.1.4. The creation date of the registration;*
> *4.3.1.5. The expiration date of the registration;*
> *4.3.1.6. The name, postal address, e-mail address, telephone number, and(wherever available) fax number of the registrant for the Registered Name;*
> *4.3.1.7. The name, postal address, Aadhaar Card, PAN Number, e-mail address, telephone number, and (wherever available) fax number of the technical contact for the Registered Name;*
> *4.3.1.8. The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.*
> *4.3.1.9. The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the billing contact for the Registered Name;*
>
> *4.3.2. Upon receiving any updates to the data elements listed in this Section 4.3 from the Registrant, Registrar shall promptly, and not later than three (3) business/working days, update its database and provide*

such updates to .IN Registry immediately.

4.3.3. Registrar agrees and undertakes that it shall maintain an updated ccTLD WHOIS of all its Registrants. Any non-maintenance of .IN WHOIS database shall be considered as a material breach of this agreement and .IN Registry may at its sole discretion terminate the accreditation of the Registrar and NIXI shall impose a penalty equal to five times the monthly billing amount.

4.3.5. The Registrar undertakes that it shall abide by .IN Registry directives/orders of the NIXI, if a prohibited status on any domain name is in place and the Registrar

[...]"

(d) DNRs are bound to comply with the laws, rules, regulations, and administrative notifications/orders etc., issued by NIXI and Indian Governmental agencies concerning the internet and NIXI.

(e) In terms of clause 4.4.3 of the (hereinafter "*the NIXI Agreement*") anonymous or proxy registrations is disallowed. The information about the Registrant or the Administrative Contact has to be reflected and no privacy or proxy services would be provided by any DNR of '.in' or '.bharat' domain name. Any violation of the said provision will constitute a material breach of the (hereinafter "*the NIXI Agreement*"). The said clause reads as under:

"4.4.3. Registrars shall not accept anonymous or "proxy" registrations nor shall they include information in the domain name registration for the "Registrant" or "Administrative Contact" fields that do not reflect the true registered domain name holder or administrative contact. No privacy or proxy service will be provided by any Registrar of .IN Registry to .IN/.Bharat domain name

registrants. It is to be noted that violation of these provisions will constitute a material breach of the agreement and the Registrar/Registrant can invite termination of RAA by the NIXI along with the imposition of appropriate penalty."

(f) DNRs shall accept written complaints from third parties regarding false or inaccurate WHOIS data of Registrants.

(g) Use of temporary email addresses during the process of creating of a domain name and throughout its lifecycle by a Registrant is prohibited. The DNRs are required to implement appropriate measures to validate the authenticity of the email provided. The relevant Clause 4.4.9 of the NIXI Agreement as also the list of prohibited temporary and encrypted email providers is extracted hereunder:

"The Registry explicitly prohibits the use of temporary email addresses, as per the list available at the .IN Registry website, during the process of creating a domain name request and thereafter throughout the lifecycle. Registrants are required to provide a valid and permanent email address for communication and verification purposes. The Registrar shall implement appropriate measures to validate the authenticity of the provided email address. In the event that a temporary email address is being used, the Registry reserves the right to reject or suspend the domain name. The registrar will conduct annual verification process of email addresses and maintain a log, which will be provided to NIXI on regular basis."

S. No.	**Temporary Email Providers**	**Encrypted Email Providers**
1.	Guerrilla Mail -	ProtonMail -

	https://www.guerrillamail.com	https://proton.me/mail
2.	10 Minute Mail - https://10minutemail.com	Tutanota - https://tutanota.com
3.	Temp Mail - https://temp-mail.org	Mailfence - https://mailfence.com
4.	Mailinator - https://www.mailinator.com	Hushmail - https://www.hushmail.com
5.	EmailOnDeck - https://www.emailondeck.com	StartMail - https://www.startmail.com

(h) In terms of Clause 4.4.11. of the NIXI Agreement the DNR shall maintain record of IP logs associated with the registration and management of domain names. The same shall include the IP addresses, timestamps, and relevant activity logs of all interactions between the DNR's systems and Registrant's system. The said information shall be stored securely for a period of 90 days.

(i) The NIXI Agreement also requires all Registrants, including foreign nationals, to undergo mandatory 'electronic Know Your Customer' (e-KYC) procedures. All Registrants are required to provide accurate, authentic and verifiable identification information along with supporting documents. The DNRs are required to maintain the said information and provide the same to NIXI, if requested, within a period of 3 working days. Further, NIXI may conduct random checks on the e-KYC documents and WHOIS details provided by the Registrants.

(j) The DNR shall implement dual authentication procedure for the Registrants, whereby verification/ authentication of Registrant shall be done through verification of email address and designated contact number.

(k) The DNR shall implement and maintain technical measures to prevent the

registration of domain names through virtual private networks.

(l) DNRs shall not transmit the personal data of the Registrants from WHOIS database to third parties unless directed by NIXI, LEAs or any competent authorities of the Government of India as per the applicable laws.

Privacy Considerations vis-à-vis Disclosure Obligations:

186. The thrust of the submissions made by the DNRs, in respect of disclosure of a Registrant's information to the Plaintiffs, was on the privacy obligations mandated under the respective agreements with ICANN and Registry Operators, as also in terms of GDPR and DPDP Act.

187. It is noted by the Court that the standard Registrar Accreditation Agreement was agreed upon and adopted by ICANN in the year 2013. The said agreement and the Registry Agreement do not in any manner obligate Registry Operator or DNRs to mask the data relating to any Registrants of domain name. In fact the WHOIS Specification which is contained in the annexure to the Registry Agreement, being Specification No. 4 titled 'Registration Data Publication Services', provides for collection of complete details of the concerned DNR and the Registrant, as also the admin for the domain name, the Registrar (administrative) and Registrar (technical). This clause of the Registry Agreement is relevant and is extracted below:-

> *"1.4. WHOIS Data Directory Services.*
>
> *1.4.1 Until the WHOIS Services Sunset Date, Registry Operator will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based WHOIS Service at <whois.nic.TLD> providing free public query-*

based access to at least the following elements in the following format.

1.4.2 The format of responses shall follow a semi-free text format outlined below, followed by a blank line and a legal disclaimer specifying the rights of Registry Operator, and of the user querying the database.

1.4.3 Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.

1.4.4 For fields where more than one value exists, multiple key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.

1.4.5 The fields specified below set forth the minimum output requirements.

1.4.6 Domain Name Data

(1) Query format: whois EXAMPLE.TLD

(2)Response format:
Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example.tld
Registrar URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z

Registry Expiry Date: 2010-10-08T00:44:592
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.123551234
Reseller: EXAMPLE RESELLER1
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registry Registrant ID: 5372808-ERL
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Registry Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX

Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.TLD
Registry Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signed Delegation
DNSSEC: unsigned
URL of the ICANN WHOIS Inaccuracy Complaint Form: https://www.icann.org/wicf/"

188. This position, however, had to be modified in view of the GDPR coming into effect. Thus, after the introduction of the GDPR, 'Temporary Specification for gTLD Registration Data' (hereinafter "*Temporary Specifications*") has been adopted on 17th May, 2018 for publication of GTLD data. The said specification mandates **redaction** of the Registrant's details including the name, street, city, postal code, phone number, fax etc., as also the details of the administrative and technical contact. Only the email addresses are permitted to be published without the consent of the Registrants. This in effect has been converted into the default

mechanism by all DNRs wherein the data relating to the Registrants are completely **redacted**. This is done even without consciously obtaining consent from the concerned Registrant. Thus, as on date, for all domain name registration the details of the Registrants of the administrative contact and of the technical contact remain **redacted** and the onus is upon the registrant to consciously opt for giving consent for publication of this data. This has resulted in a situation where unscrupulous persons have taken shelter under the garb of privacy to shield themselves from action against infringing conduct. Further, the consequences of this practice have resulted in severe constraints on ICANN's ability to ensure accuracy of data provided by the Registrants, and has enhanced the difficulty for complainants to access details of the infirming domain name. This has also been acknowledged by ICANN, on its website, the relevant portion of which reads as under:

> *"Data accuracy obligations and ICANN org's enforcement of these obligations have not changed post-GDPR. However,* ***the volume of complaints has diminished significantly concurrent with personal registration data becoming unavailable following adoption of the GDPR. ICANN org and potential complainants now lack direct access to registration data as a result of the GDPR, making it much more difficult to identify instances of registration data inaccuracy or to take action to correct them****. [...]"*[11]

[11] Accessed at: https://www.icann.org/resources/pages/registration-data-accuracy-obligations-gdpr-2021-06-14-en

189. It is relevant to note that although the said Temporary Specification require the DNRs and Registry Operators to redact information of the Registrant, it also mandates that the DNRs and Registry Operators **must** provide reasonable access to the personal data in the registration data to third parties on the basis of legitimate interest pursued by the said third party. The relevant portion of the same reads as under:

> ***"4. Access to Non-Public Registration Data***
> *4.1.* ***Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to third parties on the basis of a legitimate interests pursued by the third party****, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR.*
> *4.2. Notwithstanding Section 4.1 of this Appendix, Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to a third party where the Article 29 Working Party/European Data Protection Board, court order of a relevant court of competent jurisdiction concerning the GDPR, applicable legislation or regulation has provided guidance that the provision of specified non-public elements of Registration Data to a specified class of third party for a specified purpose is lawful. Registrar and Registry Operator MUST provide such reasonable access within 90 days of the date ICANN publishes any such guidance, unless legal requirements otherwise demand an earlier implementation."*

190. In view of the above, it would be necessary to consider what would constitute legitimate interest that would mandate DNRs or Registry Operators to

disclose personal information of the Registrants registering infringing domain names. Article 6 of the GDPR lays down the grounds on which personal data may be processed and sub-paragraph (f) of Article 6(1) permits processing of personal information on the ground of legitimate interest of third party. The Article 6(1) of the GDPR is extracted hereunder:

> *"Article 6*
> *Lawfulness of Processing*
> *1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
> *(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
> *(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
> *(c) processing is necessary for compliance with a legal obligation to which the controller is subject;*
> *(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
> *(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
> ***(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data,*** *in particular where the data subject is a child.*
> *Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."*

191. Ms. Kruthika Vijay, ld. Counsel appearing for Hosting Concepts has drawn the attention of the Court to the seminal decision of the Court of Justice of the European Union[12] (hereinafter "*CJEU*") in respect of interpretation of Article 7(f) of the *EU Directive 95/46/EC*[13] (similar to Article 6(f) of the GDPR). The CJEU while considering the issue whether the details of a person, who undertook a ride in a cab could be disclosed to the trolley company with which it had an accident, has laid down the tests for determining whether the disclosure of personal information is for legitimate interest. The following issues were under consideration:

> *"(1) Must the phrase 'is necessary for the purposes of the legitimate interests pursued by the ... third party or parties to whom the data are disclosed', in Article 7(f) of Directive 95/46/EC, be interpreted as meaning that the national police must disclose to Rights satiksme the personal data sought [by the latter] which are necessary in order for civil proceedings to be initiated?*
>
> *(2) Is the fact that, as the documents in the case file indicate, the taxi passenger whose data is sought by Rīgas satiksme was a minor at the time of the accident relevant to the answer to that question?"*

[12] Case C-13/16 passed by the CJEU on 4th May, 2017

[13] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 7(f) reads as: "Member States shall provide that personal data may be processed only if: […] (f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by the third party or parties to whom the data are disclosed , except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)."

192. As per the CJEU, a three pronged analysis would have to be undertaken to determine whether the processing of personal information would be permissible under Article 7(f) of the EU Directive. The said analysis include the following steps:

(i) Whether the information sought to be processed for a legitimate interest;

(ii) Whether the processing of personal information is necessary to achieve the said legitimate interest; and

(iii) Balancing the legitimate interest of the third party with the privacy rights of the concerned individual; and

Although the said case dealt with the position prior to enactment of the GDPR the above analysis has been consistently applied by CJEU when interpreting the relevant provisions of the GDPR.[14] The relevant portions of the said decision are reproduced hereunder:

> *"26. It is accordingly clear from the scheme of Directive 95/46 and from the wording of Article 7 thereof that* ***Article 7(f) of Directive 95/46 does not, in itself, set out an obligation, but expresses the possibility of processing data such as the communication to a third party of data necessary for the purposes of the legitimate interests pursued by that third party****. […]*
>
> *27. However, it should be pointed out that Article 7(f) of Directive 95/46* ***does not preclude such communication, in the event that it is made on the basis of national law****, in accordance with the conditions laid down in that provision.*
> *28. In that regard****, Article 7(f) of Directive 95/46 lays***

[14] (i) Meta Platforms and Others (General terms of use of a social network, C-252/21, EU:C:2023:537;
(ii) SCHUF A Holding (Discharge from remaining debts), C-26/22 and C-64/22, EU:C:2023:958;
(iii) Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens, C-621/22, EU:C:2024:858

down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence*.*

29. As regards the condition relating to the pursuit of a legitimate interest, as the Advocate General stated in points 65, 79 and 80 of his Opinion, ***there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest*** *(see, to that effect, judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraph 53). That analysis is supported by Article 8(2)(e) of Directive 95/46, which provides that the prohibition on the processing of certain types of personal data, such as those revealing racial origin or political opinions, is not to apply, in particular, where the processing is necessary for the establishment, exercise or defence of legal claims.*

30. As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (judgments of 9 November 2010, Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, paragraph 86; of 7 November 2013, IPI, C-473/12, EU:C:2013:715, paragraph 39; and of 11 December 2014, Ryneš, C-212/13, EU:C:2014:2428, paragraph 28). In that regard, ***according to the***

> ***information provided by the national court, communication of merely the first name and surname of the person who caused the damage does not make it possible to identify that person with sufficient precision in order to be able to bring an action against him. Accordingly, for that purpose, it is necessary to obtain also the address and/or the identification number of that person***.
>
> *[...]*
>
> *33. It follows from the foregoing considerations that Article 7(f) of Directive 95/46 must be interpreted as not imposing the obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However,* ***Article 7(f) of that directive does not preclude such disclosure on the basis of national law."***

193. Thus, as per CJEU, it is the settled position that the interest of a third party in obtaining personal information of an individual for initiating legal action against the said individual in respect of damage caused to the property of the third party would constitute as legitimate interest. Further, in respect of the factual issue before the CJEU, it was held that mere providing of first and second name of the individual would not be sufficient for identification. Accordingly, the address or identification number of the individual would also be necessary.

194. A conjoint reading of the above position *qua* legitimate interest and an analysis of the sample agreements discussed above, it is clear that while respect has to be given to privacy, the same need not be as a default position. Moreover,

any third party who has a legitimate interest can always approach the DNR or the Registry Operator and obtain the access to the personal data in the registration data. This obligation as contained in Clause 4.1 of the Temporary Specifications in the Registry Agreement between ICANN and Registry Operators clearly shows that even where there is privacy protect, timely providing of data is a necessary obligation in pursuance of the legitimate interest.

New Registration Data Policy

195. At this stage it would be relevant to note that further modifications have been implemented by ICANN to the policy in respect of collection, storing, publication and disclosure of personal data of the Registrant. The said Registration Data Policy has been brought into effect by ICANN from 21st August, 2025 and is applicable to all Registry Operators and DNRs having agreements with ICANN. The said policy has been introduced to take into account not only the mandate of the GDPR but also the requirements of other privacy regulations. It would be necessary to mention the important provisions of the said policy having bearing on the issues at hand, and the same are as under:

(i) The DNRs are mandated to collect the following information:

"6.1.1Domain Name

6.1.2. Registrar Whois Server*

6.1.3. Registrar URL*

6.1.4. Registrar*

6.1.5. Registrar IANA ID*

6.1.6. Registrar Abuse Contact Email*

6.1.7. Registrar Abuse Contact Phone*

6.1.8. Domain Status(es)*

6.1.9. Registrant Name

6.1.10. Registrant Street

6.1.11. Registrant City

6.1.12. Registrant State/Province

6.1.13. Registrant Postal Code

6.1.14. Registrant Country

6.1.15. Registrant Phone

6.1.16. Registrant Email

6.1.17. Registrar Registration Expiration Date*"

(ii) In response to a request for information, the DNRs and Registry Operators **must** publish the following data elements:

"9.1.1.1. Domain Name

9.1.1.2. Registrar URL

9.1.1.3. Creation Date

9.1.1.4. Registry Expiry Date (exception: Registrar MAY Publish)

9.1.1.5. Registrar Registration Expiration Date (exception: Registry Operator MAY Publish)

9.1.1.6. Registrar

9.1.1.7. Registrar IANA ID

9.1.1.8. Registrar Abuse Contact Email

9.1.1.9. Registrar Abuse Contact Phone

9.1.1.10. Domain Status(es)

9.1.1.11. Last Update of RDDS"

(iii) In addition to the above information publication of which is mandatory, the following information **must** also be published, subject to the redaction requirements provided under Section 9.2 of the Policy:

"9.1.6.1. Registrant Name

9.1.6.2. Registrant Street

9.1.6.3. Registrant City

9.1.6.4. Registrant Phone

9.1.6.5. Registrant Email"

(iv) The Section 9.2 of the Policy requires the Registry Operators and DNRs to redact the certain information provided by the Registrants where it required to comply with applicable law. Further, the redaction of information may also be done where for either a commercially reasonable purpose or where technically it is not feasible to limit application of the Section 9.2 of the Policy. The following data elements must be redacted where the Registry Operator or DNRs are applying the requirements of Section 9.2:

"9.2.2.1.1. Registry Domain ID

9.2.2.1.2. Registry Registrant ID

9.2.2.1.3. Registrant Name

9.2.2.1.4. Registrant Street

9.2.2.1.5. Registrant Postal Code

9.2.2.1.6. Registrant Phone

9.2.2.1.7. Registrant Phone Ext

9.2.2.1.8. Registrant Fax

9.2.2.1.9. Registrant Fax Ext

9.2.2.1.10. Registry Tech ID

9.2.2.1.11. Tech Name

9.2.2.1.12. Tech Phone

9.2.2.2.1. Registrant Email

9.2.2.2.2. Tech Email"

(v) Section 9.2.4 of the Policy expressly mandates the DNRs where redacting the information mentioned above, to provide the opportunity to the Registrant to provide its consent to publish the said information. Further, the DNRs must publish the information for which consent has been provided by the Registrant.

(vi) Where an affiliated or accredited privacy or pry service has been used by the Registrant, the DNRs and Registry Operators must publish the full registration data of the said privacy or proxy service.

(vii) Section 10 of the Policy provides for the procedure for disclosure of information collected by the DNRs and Registry Operators in respect the domain names. The said section requires a proper Disclosure Request be made by the third party in the format set by DNRs and Registry Operators, which must include the following:

"10.2.1. The identity of the requestor, including:

10.2.1.1. The contact information of the requestor,

10.2.1.2. The nature/type of business entity or individual, and

10.2.1.3. Power of Attorney statements or similar statements evidencing authorization to act on the requestor's behalf, where applicable and relevant.

10.2.2. A list of data element values requested by the requestor.

10.2.3. Information about the legal rights of the requestor and specific rationale and basis for the request.

10.2.4. An affirmation that the request is being made in good faith.

10.2.5. Agreement by the requestor to process lawfully any data element values received in response to the request."

(viii) The DNRs or Registry Operator must acknowledge every request in proper format within two days, and must respond to the same after considering it on merits within 30 days from the date of acknowledgement. The response to the disclosure request must be in either of the following ways:

"10.6.1. Provide the requested data; or

10.6.2. ***Provide rationale for why Registry Operator or Registrar cannot provide the requested data (in whole or in part) that identifies the specific reason(s) for such denial, including a clear explanation of how it arrived at its decision that is sufficient for a requestor to objectively understand the reasons for the decision. This includes an analysis and explanation of how the fundamental rights and freedoms of the data subject were weighed against the legitimate interest of the requestor (if applicable)."***

(ix) The Registry Operator or the DNRs are not prohibited from processing of data for other purposes which are beyond the scope of the Policy, including collection or generation of additional data elements in order to create a contact. The same must be published after obtaining consent of the Registrant.

196. Thus, it is clear from the above enumerated changes in the privacy policy that the DNRs and Registry Operators cannot deny disclosure of Registrant's details by taking blanket cover under the provisions of GDPR. The applicable privacy law would govern the relevant considerations in each case, and accordingly, the data collected from Registrants in India would be governed in terms of the DPDP Act and its allied Rules.

197. It would also be relevant to consider the decision of this Court in ***Neetu Singh & Anr. vs. Telegram FZ LLC & Ors., 2022:DHC:3333*** (decided on 30th August, 2022), wherein the decision of the Supreme Court in ***Justice K.S. Puttaswamy & Anr. v. Union of India & Ors., (2017) 10 SCC 1***, has been relied upon in respect of lawful disclosures that can be made in respect of IP infringement. Although the said case dealt with Copyright infringement the observation therein would be relevant:

> *"45. This brings the Court to the defences taken by Telegram in its response to the prayer for disclosure. In this regard, this Court finds as under:*
>
> *(i)[...]*
>
> *xi) In this vein, Telegram also relied upon the judgement of the Supreme Court in Puttaswamy (supra). The relevant extract of the said decision reads as under:*
>
> *"310. While it intervenes to protect legitimate State interests, the State must nevertheless put into place a robust regime that ensures the fulfilment of a threefold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). They emanate from the procedural and content-based mandate of Article 21.* ***The first requirement that there must be a***

law in existence to justify an encroachment on privacy is an express requirement of Article 21. *For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law. The existence of law is an essential requirement.* ***Second, the requirement of a need, in terms of a legitimate State aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary State action****. The pursuit of a legitimate State aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. Judicial review does not reappreciate or second guess the value judgment of the legislature but is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness.* ***The third requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary State action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the threefold requirement for a valid law arises out of the mutual interdependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty, on the other.*** *The right to privacy, which is an intrinsic part of the right to life and liberty, and the freedoms embodied in Part III is subject to the same restraints which apply to those freedoms.*

xxx xxx xxx

328. Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can

originate not only from the State but from non-State actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union Government while designing a carefully structured regime for the protection of the data. Since the Union Government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union Government having due regard to what has been set out in this judgment."

As per the above extract from K.S. Puttaswamy (supra) it is clear that the Supreme Court recognises that if there is a law in existence to justify the disclosure of information and there is a need for the disclosure considering the nature of encroachment of the right then privacy cannot be a ground to justify non-disclosure, so long as the same is not disproportionate. In India, the Copyright Act is clearly a law, which requires "infringing copies" to be taken into custody. The Copyright Act recognizes the right of the copyright owner to claim damages and rendition of accounts in respect of such infringement. Secondly, whenever the data is sought for a legitimate purpose, and for curbing the violation of law, including infringement of copyright, the same would be in accordance with the legal position recognised in K.S. Puttaswamy (supra)."

198. Thus, it is the settled position that disclosure of personal information would have to satisfy the three-fold test *i.e.,* (i) the disclosure must be made in terms of a law justifying the encroachment of privacy, (ii) the said law must be pursuant to a legitimate aim of the State; (iii) means for disclosure are proportional to the legitimate aim sought to be achieved. This is similar to the three factors considered under the EU regime discussed above.

199. Indian laws i.e., the DPDP Act along with the DPDP Rules, 2023, notified on 14th November, 2025, satisfy the first requirement of the existence of law regulating disclosure of personal information. Under Section 4 of the DPDP Act processing of personal information may only happen where either the data fiduciary has given her consent or for certain legitimate uses provided under Section 7 of the said Act. Section 7 of the DPDP Act reads as under:

> *"7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:—*
>
> *(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data. […]*
>
> *(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;*
>
> *(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the*

provisions regarding disclosure of such information in any other law for the time being in force;

(e) ***for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India****;[…]"*

200. Thus, as per the above a DNR will have to disclose the details of the Registrant of an infringing domain name upon a direction in this regard being issued by the Indian Courts. It is also relevant to note that ICANN in fact has contemplated the possibility of different national laws preventing the DNRs or Registry Operators from complying with the provisions of the agreements with ICANN.[15]

201. Having discussed the relevant agreements between ICANN and DNRs as also Registry Operators, the Court is of the view that several significant obligations have been imposed upon the said parties to ensure that registration of a domain name does not violate the rights of a third party. On one hand, the Registry Operators must comply with ICANN's policies, bye-laws, and the codes of conduct. They are required to operate the WHOIS services in the format prescribed in Specification 4, along with observing reserved names listed in Specification 5. They are obligated to take reasonable steps to investigate and respond to requests from law-enforcement or governmental bodies regarding illegal conduct involving their TLDs. They must additionally implement Rights Protection Mechanisms under Specification 7, including use of the Trademark

[15] https://www.icann.org/en/contracted-parties/accredited-registrars/resources/whois-privacy-law-conflicts

Clearinghouse database, which alerts both registrants and trademark owners when a domain identical to a recorded trademark is sought to be registered, enabling early detection of potential trademark conflicts.

202. Further, DNRs under these frameworks discussed above, must submit registered-name data to the Registry Operator, provide public query-based access to essential WHOIS/RDDS information, make registrant data available for ICANN's inspection, comply with applicable laws and governmental regulations, avoid registering reserved names, verify and periodically re-verify Registrant contact information, investigate inaccuracies, and act promptly against DNS abuse or illegal activity. They face termination of the accreditation agreement if a Court finds they permitted illegal activity or failed to comply with Court's orders, or if ICANN determines that the DNRs engaged in bad-faith trademark-conflicting registrations. Additionally, they must follow ICANN's WHOIS Accuracy Specification, validating address, email, and phone formats, and verifying email or telephone numbers through tool-based authentication, and must suspend or terminate domain names where registrants wilfully provide inaccurate information and fail to correct it within 15 days.

203. However, in the experience of the Court in adjudicating these matters as also in view of the provisions under the NIXI Accreditation Agreement, either the Registry Operators and DNRs are not complying the abovementioned obligations or the same are not sufficient to safeguard the rights of trademark owners in India. These measures in the opinion of this Court appear to have fallen short, by significant degree, since not only do the permitted unscrupulous Registrants continue to infringe the rights of various trademark owners, but are

also defrauding numerous innocent persons, by taking shelter under the Privacy policies of the DNRs which mask the registrant's details.

Modus Operandi of the Registrants of Infringing Domain Names

204. The present batch of suits under consideration by this Court had been filed initially against some infringing domain names, after including the DNRs who had registered the concerned domain names for certain third parties. The identity of those persons or their contact details is not evident from the WHOIS details available on the respective DNR's website or the WHOIS database due to *'privacy by default'* implemented by the DNRs due to which the same have been redacted. Further, in various suits the said details have not been disclosed to the plaintiffs, despite the clear legitimate interest of the said parties. It has become evident during the course of these proceedings that these domain names have been registered by unknown persons mostly with fake address, mobile numbers, email addresses and details which are either fictitious or wholly incorrect. The only available contact detail is the email address, if the same has not been redacted, from which also it is almost impossible to decipher as to who is the person or entity who has registered the infringing domain name. Examples of few such false and fictitious registration details placed on record by the Plaintiff are as follows:

2025:DHC:11874

Whois
Identity for everyone

HOME DOMAINS WEBSITES HOSTING CLOUD EMAIL SECURITY WHOIS

colgatepalmolive.in

Updated 21 hours ago

Domain Information

Domain:	colgatepalmolive.in
Registrar:	GoDaddy.com, LLC
Registered On:	2019-05-06
Expires On:	2020-05-06
Updated On:	2019-05-06
Status:	clientRenewProhibited clientTransferProhibited clientUpdateProhibited clientDeleteProhibited addPeriod
Name Servers:	ns55.domaincontrol.com ns56.domaincontrol.com

Registrant Contact

State:	Uttar Pradesh
Country:	IN
Email:	Please contact the Registrar listed above

Administrative Contact

Email:	Please contact the Registrar listed above

Technical Contact

Email:	Please contact the Registrar listed above

Raw Whois Data

```
Domain Name: colgatepalmolive.in
Registry Domain ID: D9DAF2C8727AF4AAAAB16983A1E9F5ED0-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2019-05-06T06:48:39Z
Creation Date: 2019-05-06T06:48:38Z
Registry Expiry Date: 2020-05-06T06:48:38Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProh
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibit
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibit
Domain Status: addPeriod http://www.icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant Street:
Registrant Street:
```

2025:DHC:11874

Whois Record for ColgateIndia.in

– Domain Profile

Registrar	GoDaddy.com, LLC IANA ID: 146 URL: www.godaddy.com Whois Server: –
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	128 days old Created on 2023-06-12 Expires on 2024-06-12 Updated on 2023-06-17
Name Servers	NS49.DOMAINCONTROL.COM (has 60,676,335 domains) NS50.DOMAINCONTROL.COM (has 60,676,335 domains)
IP Address	3.33.130.190 - 28,915,475 other sites hosted on this server
IP Location	- New Jersey - Princeton - Amazon Technologies Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
IP History	1 change on 1 unique IP addresses over 0 years
Hosting History	3 changes on 3 unique name servers over 3 years

Whois Record (last updated on 2023-10-18)

```
Domain Name: colgateindia.in
Registry Domain ID: D56E98C6F36364F37A69320AE4B6C8C05-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2023-06-17T10:52:05Z
Creation Date: 2023-06-12T10:52:04Z
Registry Expiry Date: 2024-06-12T10:52:04Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibite
d
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibite
d
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhi
bited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
```

//TRUE COPY//

```
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Delhi
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns50.domaincontrol.com
Name Server: ns49.domaincontrol.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

For more information on Whois status codes, please visit https://icann.org/epp
```

Moreover, the giving of fake addresses by any registrants ought to be avoided by putting a proper technology in place to verify that there is some authenticity in the address.

205. As is evident from the above, in case of most domain name registrations the details are redacted by the DNRs, and where the same are available publicly, the details are either grossly incorrect and not sufficient by any means for identification to initiate legal actions against the same. As an illustration, it is interesting to see that in the lead matter *i.e.,* ***Dabur India (supra),*** the details of the Registrant of one of the infringing domain names therein *i.e.,* **daburdistributor.com,** against which an injunction order had been passed and the concerned DNR had been asked to provide the same to the Plaintiff. A perusal of the said details would show that the address mentioned is the same address as that of the Plaintiff therein (*i.e., Dabur India Limited)* being ***8/3, Asaf Ali Road, New Delhi -110002,*** and the details provided by the concerned DNR are as under:

Document C

Domain Name daburdistributor.com
Registered On 2020-08-20 06:07:24+00
Expiry 2022-08-20 06:07:24+00
PP Enabled false
Registrar PDR Ltd. d/b/a PublicDomainRegistry.com
Nameservers ns1.suspended-domain.com
ns2.suspended-domain.com
Reseller Lock f
Theft Protection t
RAA Verification Status
Name Dabur Distributor
Company Dabur Distributor
Email info.daburdistributor@gmail.com
Address 83, Asaf Ali Road,,
City New Delhi
State Delhi
Country IN
Zip 110002
Tel No 91-7296084305

The address provided above is the address of the Plaintiff and not the Registrant. Thus, there is no doubt that the DNRs are completely failing in the obligation to verify the accuracy of the details provided by the Registrants.

206. It is also clear that this information is available only with the DNRs who collect the email address from the party registering the domain names. Most of the remaining details given to the DNRs are also fake such as addresses and mobile numbers. There are no other verification standards adopted for verifying the identity of the persons registering the domain names. Hence, even if the email address is provided, a second enquiry is required to find out as to who has created this email address. On most occasions email addresses are created by using short duration mobile numbers or accessing from cyber cafes. The BIS data would also reveal that such registrants may be located in foreign shores. **Thus, merely with**

the email address of the Registrant of the domain name, it is almost impossible to trace the person who has registered it.

207. The necessity of obtaining accurate and reliable information from the Registrants of domain names has been recognised and acknowledged by WIPO in the following terms:

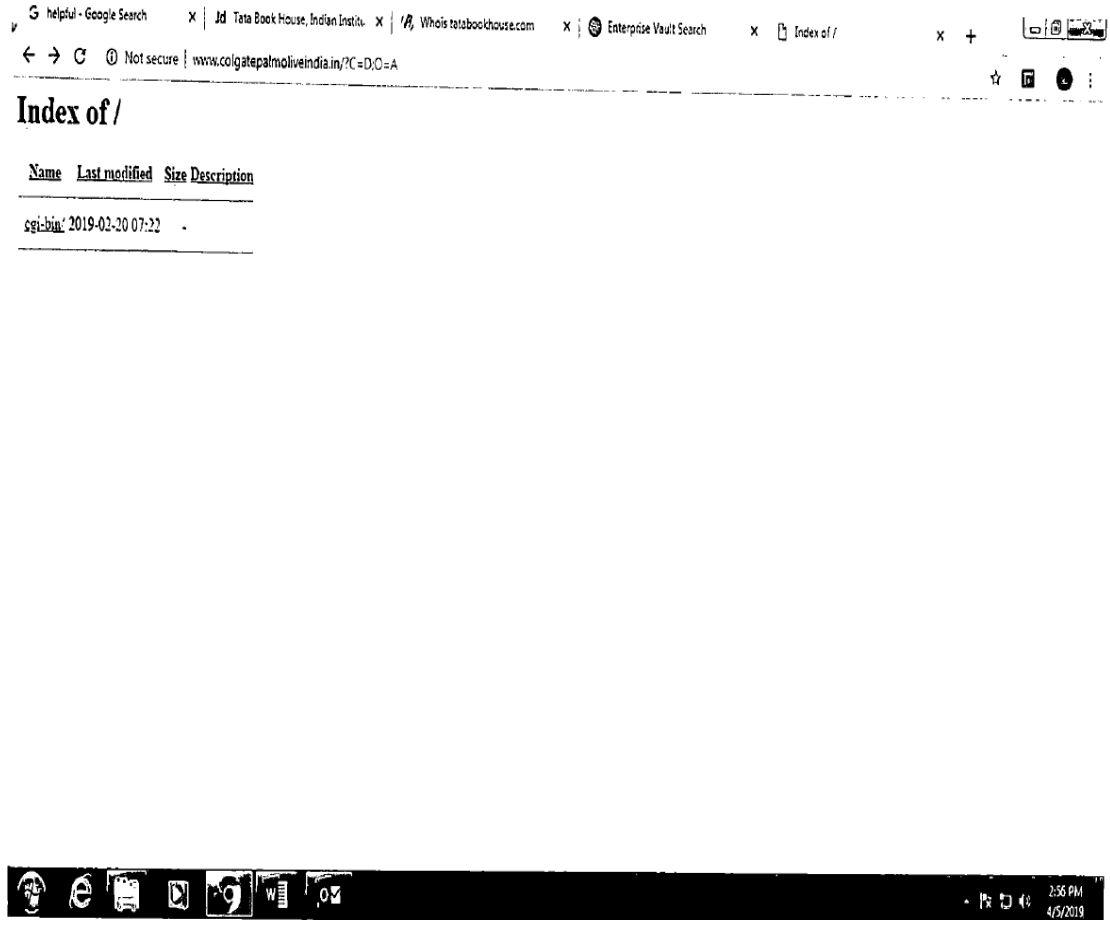
> *"64. In the WIPO Interim Report, it was recommended that the domain name registration agreement contain a requirement that the domain name applicant provide certain specified contact details. The collection (as opposed to the availability) of contact details by registrars is the least controversial aspect of the discussion on contact details.* ***We consider that it is essential for the legitimate protection and enforcement of intellectual property rights, as well as for many other public policies recognized in the law, that contact details be collected. Without accurate and reliable contact details, the task of assigning responsibility for activities on the Internet is vastly complicated.*** *Other means of assigning responsibility for activities on the Internet do exist.* ***Where it is sought to enforce a criminal law, for example, the apparatus of the State can be activated to use tracing and other measures to determine the origin of activities, although, even here, the cross-border nature of the Internet complicates the task.*** *In respect of civil law enforcement, however, the task of activating the apparatus of the State to identify responsibility for activities is more difficult.*
>
> *65. ICANN's Statement of Registrar Accreditation Policy adopts the draft recommendation in the WIPO Interim Report and requires registrars to oblige domain name applicants to provide accurate and reliable contact*

details."[16]

208. After obtaining the domain name registration and hiding the contact details, the Registrants use web developers or develop the infringing websites on their own. In most cases the content of the trademark owner's website is replicated. In addition, job offers, franchisees, dealerships are offered. When innocent users or members of the public believe these websites to be true and genuine, payments are made to the bank accounts reflected on the website. They realise soon thereafter that the entire process was a fake. The bank accounts which are opened are in the names of John Does and have no connection with the trademark owner or the brand owner. When payments are made through RTGS or NEFT, the name of the recipient who is holding the bank account is not visible hence the person paying the money has no way of realising that the amount is in fact being credited not to the trademark owner or to the well-known company but to some unscrupulous individual or entity. In the present case, it the Registrants of the infringing domain names have been using the trade mark and brand name of the Plaintiffs to defraud innocent individuals by asking for deposit of money in respect of fake interviews. Further, the website linked with the said email ids are non-functional clearly showing the intention of the concerned Registrants to misuse the said domain name. Some screenshots of infringing websites, the emails received by innocent persons along with the fake interview letter are set out below:

[16] Final Report of the First WIPO Internet Domain Name Process, April 30, 1999.

2025:DHC:11874


helpful - Google Search | Tata Book House, Indian Institu | Whois tatabookhouse.com | Enterprise Vault Search | Index of /

Not secure | www.colgatepalmoliveindia.in/?C=D;O=A

Index of /

Name	Last modified	Size	Description
cgi-bin/	2019-02-20 07:22	-	

2025:DHC:11874

---------- Forwarded message ---------
From: **COLGATE PALMOLIVE** <info@colgatepalmolive.in>
Date: Tue, 7 May, 2019, 9:18 PM
Subject: **An Invitation For the Interview **
To:

Dear Candidate,

TRUE COPY

74

We, at Colgate Palmolive (INDIA) Ltd. were pretty impressed by the profile of yours. After careful reviewing of the profile, we have decided to call you for a personal interview to finalize our decision and to tell you more about what we do and would also like to get to know you better.

We would like to invite you to come at our office for Interview.

your interview has been scheduled for ,May 16, 2019, 10:30 AM,

Office- 2nd Floor, Tower 3A DLF Corporate Park, M.G. Road Gurugram 122002 .
If the date or time of the interview is inconvenient, you can contact by phone between 10 AM to 6 PM (+91-7065828937) in order to arrange another appointment.

We look forward to seeing you.

Regards,

V.K.Jain

Human Resource Dept Head

Note- Find Your attachment, We have attached your Call Letter with all terms and Conditions..

2025:DHC:11874

82
22

COLGATE-PALMOLIVE

Colgate

COLGATE PALMOLIVE INDIA. LTD

Ref No. COLPALMIVE/770742/578287P **Dated :- 01/03/2019**

Dear Candidate,

We are glad to inform you that you have been selected on behalf of your resume for an HR interview in our company by our direct recruitment cell. We have short listed "48" fresh and experience candidates for "35" vacancies in **"Sales & Marketing, Human Recourses, Financial strategy, Logistic and Operations Manufacturing & Production "** in India and Abroad.

As your resume is found satisfactory, we are inviting you for an interview at our company HR office. Place and time of your venue are as per follows:

Date of Venue	:	**25/03/2019**
Venue of Interview	:	**2nd Floor Tower 3A DLF Corporate Park Near Guru Dronacharya Metro Station M.G. Road, Gurugram-122002**
Time	:	**10 : 30 A.M.**

You will have to come with the following documents for attending the interview:

- Hard copy of Invitation mail.
- Mark sheets & Certificates of 10th & 12th mark sheet & Degree certificates of graduation and post-graduation.
- Diploma holders could come along with the degree or diploma and other qualification certificates.
- Candidates those who are pursuing their or diploma could come along for this interview. They could submit their degree or diploma after completion of their course. (If selected).
- Passport (For those candidates who are willing to go abroad).

Candidates coming late will not be allowed.

Salary offered for these posts varies between 39,700 /- to 2,20,000 /- INR. (HRA + D.A &other benefits).

Air/Train tickets according to the location of the candidates & accommodation will be provided by the company.

One extra person is allowed with Female candidate. Tickets for the person accompanying will also provide by the company.

NOTE :-Candidates **have to deposit a refundable security amount Rs.8,750/- by Cash/NEFT/RTGS/IMPS into the STATE BANK OF INDIA.**

REOSON FOR SECURITY DEPOSIT- Company is not taking any charge from any candidates it's just for surety that candidate will not skip there interview and company can provide the air tickets and other expenses for candidates.

Last date security deposit t is **12/03/2019** .Your call latter and air ticket will dispatch very shortly after receiving your confirmation of security deposited in the Bank.

Security amount will be refunded to all the candidates after the interview without any deduction.

Brief job description will be mentioned in the hall tickets. Air/Hall tickets will be mailed to the candidates soon after receiving confirmation mail of counterfoil and details by respective candidates.

Note : Candidates are invited to their location, eligibility and our requirements.

Refundable security amount is just the security amount to ensure that if the company is providing you the tickets, candidate should be present at the time of interview.

Hope that you will accept this job offer and looking forward to welcome you India and abroad for this interview.

Regards

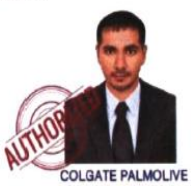
Senior HR

Mr. Vishal Sharma

Mr. Vishal Sharma

+91- 7065743695

TRUE COPY



COLGATE PALMOLIVE
INDIA LIMITED.

2025:DHC:11874

75

COLGATE-PALMOLIVE

Colgate

COLGATE PALMOLIVE INDIA. LTD

Ref No. COLPALMIVE/770742/578287P

Dated :- 01/05/2019

Dear Candidate,

We are glad to inform you that you have been selected on behalf of your resume for an HR interview in our company by our direct recruitment cell. We have short listed "48" fresh and experience candidates for "35" vacancies in **"Sales & Marketing, Human Recourses, Financial strategy, Logistic and Operations Manufacturing & Production "** in India and Abroad.

As your resume is found satisfactory, we are inviting you for an interview at our company HR office. Place and time of your venue are as per follows:

Date of Venue	:	**16/05/2019**
Venue of Interview	:	**2nd Floor Tower 3A DLF Corporate Park Near Guru Dronacharya Metro Station M.G. Road, Gurugram-122002**
Time	:	**10 : 30 A.M.**

You will have to come with the following documents for attending the interview:

- Hard copy of Invitation mail.
- Mark sheets & Certificates of 10th & 12th mark sheet & Degree certificates of graduation and post-graduation.
- Diploma holders could come along with the degree or diploma and other qualification certificates.
- Candidates those who are pursuing their or diploma could come along for this interview. They could submit their degree or diploma after completion of their course. (If selected).
- Passport (For those candidates who are willing to go abroad).

Candidates coming late will not be allowed.

Salary offered for these posts varies between 39,700 /- to 2,20,000 /- INR. (HRA + D.A &other benefits).

Air/Train tickets according to the location of the candidates & accommodation will be provided by the company.

One extra person is allowed with Female candidate. Tickets for the person accompanying will also provide by the company.

NOTE :- Candidates have to deposit a refundable security amount Rs.8,750/- by Cash/NEFT/RTGS/IMPS into the State Bank Of India .

REASON FOR SECURITY DEPOSIT – Company is not taking any charge from any candidate it's just for the surety that candidate will not skip there interview and company can provide the air tickets and other expenses for candidate.

Last date security deposit is **08/05/2019**, Your call letter and air ticket will dispatch very shortly after receiving your confirmation of security deposited in the Bank.

Security amount will be refunded to all the candidates after the interview without any deduction.

Brief job description will be mentioned in the hall tickets. Air/Hall tickets will be mailed to the candidates soon after receiving confirmation mail of counterfoil and details by respective candidates.

Note : Candidates are invited to their location, eligibility and our requirements.

Refundable security amount is just the security amount to ensure that if the company is providing you the tickets, candidate should be present at the time of interview.

Hope that you will accept this job offer and looking forward to welcome you India and abroad for this interview.

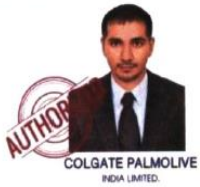
Regards

Senior Hr

V. K. Jain

+91- 7065828937

TRUE COPY



COLGATE PALMOLIVE
INDIA LIMITED.

209. These domain names and websites have thus become engines for large scale deception depriving thousands of persons of their hard-earned money in effect constituting a new form of cyber fraud.

210. In view of the above, it is clear that the measures alleged by the DNRs and Registry Operators to be set in place for protecting the rights of trademark owners are not sufficient for the said purpose. Further, taking advantage of the present practices of DNRs and Registry Operators, the errant Registrants have registered infringing domain names and defrauded numerous individuals. Accordingly, in the opinion of the Court, strict actions would have to be taken to curb the same and protect trademark rights of the plaintiffs.

ISSUE II: WHAT MEASURES MAY BE DIRECTED BY THE COURT TO BE IMPLEMENTED BY DNRS AND REGISTRY OPERATORS TO SAFEGUARD THE TRADEMARK RIGHTS OF THE PLAINTIFFS?

211. It would be relevant to consider the trademark rights of the Plaintiffs in the domain names before discussing the necessary measures for protection of the same.

Rights of Trademark Owners in Domain Names

212. In this batch of suits, there are a large number of trademarks that are sought to be enforced and protected such as Tata Sky, Amul, Bajaj Finance, Dabur, Meesho, Croma, Colgate, Colgate Palmolive, ITC, Mont Blanc etc. These trademarks have been in use for several years, are also registered trademarks, and some of them have also been recognised as *well-known marks*. The use of

these trademarks as part of domain names would constitute infringement of the Plaintiffs' statutory rights as also common law rights. Apart from the Plaintiffs' rights in the respective marks which are also likely to be diluted due to fraudulent use, the rights of the general public are also being violated. The misuse of well-known marks, brands and logos as also the names of the Plaintiffs is resulting in innocent members of the public being duped and conned into believing that the activities run under these domain names, either in the form of websites or otherwise, are being offered by the actual Plaintiffs. These fake websites through deceptive and misleading advertising are promoting their illegal and nefarious activities. Thus, apart from intellectual property rights of the Plaintiffs there is a larger public interest also that is being affected.

213. One of the arguments made on behalf of GoDaddy is that mere registration of a domain name would not amount to infringement of trademark, until and unless the said domain name is used for an infringing website or for any other illegal activity. It was argued that the DNRs cannot presumptively maintain a check in respect of well-known marks without any adjudication from the Court as to whether the subject domain names is infringing the said well-known mark. However, these legal propositions are unfounded as it is well settled legal position that registration of an infringing domain name itself constitutes a violation of rights, since domain names are recognised as worthy of trademark protections. This is clear from a perusal of the seminal decision of the Supreme Court in ***Satyam Infoway Ltd. v. Siffynet Solutions (P) Ltd., (2004) 6 SCC 145*** wherein Justice Ruma Pal – penning the Judgement for the Court, observed as under:

*"**11.** Analysing and cumulatively paraphrasing the relevant parts of the aforesaid definitions, **the question which is apposite is whether a domain name can be said to be a word or name which is capable of distinguishing the subject of trade or service made available to potential users of the internet**.*

12.** The original role of a domain name was no doubt to provide an address for computers on the internet. But the internet has developed from a mere means of communication to a mode of carrying on commercial activity. **With the increase of commercial activity on the internet, a domain name is also used as a business identifier. Therefore, the domain name not only serves as an address for internet communication but also identifies the specific internet site. In the commercial field, each domain-name owner provides information/services which are associated with such domain name. Thus a domain name may pertain to provision of services within the meaning of Section 2(1)(z).** A domain name is easy to remember and use, and is chosen as an instrument of commercial enterprise not only because it facilitates the ability of consumers to navigate the internet to find websites they are looking for, but also at the same time, serves to identify and distinguish the business itself, or its goods or services, and to specify its corresponding online internet location [Ryder, Rodney D.: Intellectual Property and the Internet, pp. 96-97.] . Consequently a domain name as an address must, of necessity, be peculiar and unique and **where a domain name is used in connection with a business, the value of maintaining an exclusive identity becomes critical.

> *"As more and more commercial enterprises trade or advertise their presence on the web, domain names have become more and more valuable and the*

potential for dispute is high. Whereas a large number of trade marks containing the same name can comfortably coexist because they are associated with different products, belong to business in different jurisdictions, etc., the distinctive nature of the domain name providing global exclusivity is much sought after. The fact that many consumers searching for a particular site are likely, in the first place, to try and guess its domain name has further enhanced this value [See Rowland, Diane and Macdonald, Elizabeth: Information Technology Law, 2nd Edn., p. 521.] ."

The answer to the question posed in the preceding paragraph is therefore in the affirmative.

[…]

16**. **The use of the same or similar domain name may lead to a diversion of users which could result from such users mistakenly accessing one domain name instead of another**. This may occur in e-commerce with its rapid progress and instant (and theoretically limitless) accessibility to users and potential customers and particularly so in areas of specific overlap. **Ordinary consumers/users seeking to locate the functions available under one domain name may be confused if they accidentally arrived at a different but similar website which offers no such services. Such users could well conclude that the first domain-name owner had misrepresented its goods or services through its promotional activities and the first domain-owner would thereby lose its custom. It is apparent, therefore, that a domain name may have all the characteristics of a trade mark and could found an action for passing off.

17. *Over the last few years the increased user of the internet has led to a proliferation of disputes resulting in litigation before different High Courts in this country.* ***The courts have consistently applied the law relating to passingoff to domain name disputes. Some disputes were between the trade-mark holders and domain-name owners.*** *Some were between domain-name owners themselves. These decisions, namely, Rediff Communication Ltd .v. Cyberbooth [AIR 2000 Bom 27] , Yahoo Inc. v. Akash Arora [(1999) 19 PTC 201 (Del)] , Dr. Reddy's Laboratories Ltd. v. Manu Kosuri [2001 PTC 859 (Del)] , Tata Sons Ltd. v. Manu Kosuri [2001 PTC 432 (Del)] , Acqua Minerals Ltd. v. Pramod Borse [2001 PTC 619 (Del)] and Info Edge (India) (P) Ltd. v. Shailesh Gupta [(2002) 24 PTC 355 (Del)] correctly reflect the law as enunciated by us.* ***No decision of any court in India has been shown to us which has taken a contrary view. The question formulated at the outset is therefore answered in the affirmative and the submission of the respondent is rejected.***

[…]

23. *These rules indicate that the disputes may be broadly categorised as: (a) disputes between trade-mark owners and domain-name owners, and (b) between domain-name owners inter se. What is important for the purposes of the present appeal is the protection given to intellectual property in domain names. A prior registrant can protect its domain name against subsequent registrants.* ***Confusing similarity in domain names may be a ground for complaint and similarity is to be decided on the possibility of deception amongst potential customers.*** *The defences available to a complaint are also substantially*

similar to those available to an action for passing off under trade mark law.

***24.** Rule 4(k) provides that the proceedings under the UDNDR Policy would not prevent either the domain-name owner/registrant or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution, either before proceeding under ICANN's policy or after such proceeding is concluded.*

***5.** As far as India is concerned, there is no legislation which explicitly refers to dispute resolution in connection with domain names. But although the operation of the Trade Marks Act, 1999 itself is not extraterritorial and may not allow for adequate protection of domain names, this does not mean that domain names are not to be legally protected to the extent possible under the laws relating to passing off."*

214. The above decision clearly holds that registration of an infringing domain name would not be permissible as there is every likelihood that the same could be led to diversion of users from the genuine website to the infringing one.

215. As is the settled position in law, actual infringement or passing off is not required to be shown in trademark infringement, and even a likelihood of confusion and damage is sufficient. In ***Laxmikant V. Patel v. Chetanbhai Shah*****, (2002) 3 SCC 65,** the Supreme Court has held as under:

***"12.** In Oertli v. Bowman [1957 RPC 388 (CA)] (at p. 397) the gist of passing-off action was defined by stating that it was essential to the success of any claim to passing-off based on the use of given mark or get-up that the plaintiff should be able to show that the disputed mark or get-up has become by user in the country distinctive of the plaintiff's*

goods so that the use in relation to any goods of the kind dealt in by the plaintiff of that mark or get-up will be understood by the trade and the public in that country as meaning that the goods are the plaintiff's goods. It is in the nature of acquisition of a quasi-proprietary right to the exclusive use of the mark or get-up in relation to goods of that kind because of the plaintiff having used or made it known that the mark or get-up has relation to his goods. Such right is invaded by anyone using the same or some deceptively similar mark, get-up or name in relation to goods not of plaintiff. ***The three elements of passing-off action are the reputation of goods, possibility of deception and likelihood of damages to the plaintiff.*** *In our opinion, the same principle, which applies to trade mark, is applicable to trade name.*

13. *In an action for passing-off it is usual, rather essential, to seek an injunction, temporary or ad interim. The principles for the grant of such injunction are the same as in the case of any other action against injury complained of. The plaintiff must prove a prima facie case, availability of balance of convenience in his favour and his suffering an irreparable injury in the absence of grant of injunction. According to Kerly (ibid, para 16.16) passing-off cases are often cases of deliberate and intentional misrepresentation, but it is well settled that fraud is not a necessary element of the right of action, and the absence of an intention to deceive is not a defence, though proof of fraudulent intention may materially assist a plaintiff in establishing probability of deception. Christopher Wadlow in Law of Passing-Off (1995 Edn., at p. 3.06)* ***states that the plaintiff does not have to prove actual damage in order to succeed in an action for passing-off. Likelihood of damage is sufficient****. The same learned author states that the defendant's state of mind is wholly irrelevant to the*

existence of the cause of action for passing-off (ibid, paras 4.20 and 7.15). As to how the injunction granted by the court would shape depends on the facts and circumstances of each case. Where a defendant has imitated or adopted the plaintiff's distinctive trade mark or business name, the order may be an absolute injunction that he would not use or carry on business under that name (Kerly, ibid, para 16.97).

14. *In the present case the plaintiff claims to have been running his business in the name and style of Muktajivan Colour Lab and Studio since 1982. He has produced material enabling a finding being arrived at in that regard. However, the trial court has found him using Muktajivan as part of his business name at least since 1995. The plaintiff is expanding his business and exploiting the reputation and goodwill associated with Muktajivan in the business of colour lab and photo by expanding the business through his wife and brother-in-law. On or about the date of the institution of the suit the defendant was about to commence or had just commenced an identical business by adopting the word Muktajivan as a part of his business name although till then his business was being run in the name and style of Gokul Studio. The intention of the defendant to make use of the business name of the plaintiff so as to divert his business or customers to himself is apparent.* ***It is not the case of the defendant that he was not aware of the word Muktajivan being the property of the plaintiff or the plaintiff running his business in that name, though such a plea could only have indicated the innocence of the defendant and yet no difference would have resulted in the matter of grant of relief to the plaintiff because the likelihood of injury to the plaintiff was writ large.*** *It is difficult to subscribe to the logic adopted by the trial court, as also the High Court, behind*

reasoning that the defendants' business was situated at a distance of 4 or 5 km from the plaintiff's business and therefore the plaintiff could not have sought for an injunction. In a city a difference of 4 or 5 km does not matter much. In the event of the plaintiff having acquired a goodwill as to the quality of services being rendered by him, a resident of Ahmedabad city would not mind travelling a distance of a few kilometres for the purpose of availing a better quality of services. Once a case of passing-off is made out the practice is generally to grant a prompt ex parte injunction followed by appointment of Local Commissioner, if necessary. In our opinion the trial court was fully justified in granting the ex parte injunction to the plaintiff based on the material made available by him to the court. The trial court fell in error in vacating the injunction and similar error has crept in the order of the High Court. The reasons assigned by the trial court as also by the High Court for refusing the relief of injunction to the plaintiff are wholly unsustainable.

[…]

16. *There was no delay in filing the suit by the plaintiff. The plaintiff filed the suit with an averment that the defendants were about to commit an injury to the plaintiff. The defendants took a plea that they had already commenced the business with the offending trade name without specifying actually since when they had commenced such business. This has to be seen in the background that the defendants' business earlier was admittedly being carried on in the name and style of Gokul Studio. The commencement of such business by the defendants could therefore have been subsequent to the institution of the suit by the plaintiff and before the filing of the written statement by the defendants.* ***In such a situation, on the plaintiff succeeding in making out a prima facie case, the court***

> ***shall have to concentrate on the likelihood of injury which would be caused to the plaintiff in future*** *and simply because the business under the offending name had already commenced before the filing of the written statement or even shortly before the institution of the suit would not make any difference and certainly not disentitle the plaintiff to the grant of ad interim injunction."*

216. These above legal propositions are so well entrenched and settled that they need not be revisited as they have been uniformly and consistently followed in Indian IP jurisprudence.

Responsibilities and duties of Registry Operators and DNRs

217. As is clear from the discussion of the previous issue, the Registry Operators and DNRs are woefully falling short of the implementing necessary safeguards to protect not only the rights of trademark owners, but also those of the common public. These entities, along with ICANN at the top, form part of the same pyramid wherein the entire domain name registration system is vested. However, despite the importance of the role played by them in the said system, the submissions made before this Court by all these entities, except NIXI, goes to show that none of these entities own up their responsibility for taking serious measures to prevent fraudulent activities involving trademarks, brand names, corporate house names etc., which have resulted in substantial losses to innocent public and to brand owners.

218. The Government, LEAs and regulatory authorities continue to wrestle with the Registry Operators and the DNRs, as also with ICANN at a policy level, to arrive at an expedient solution for very fundamental issues such as:

(i) Obtaining data relating to Registrant of an infringing domain name;

(ii) Implementing orders passed by the Indian Courts in respect of infringing domain names;

(iii) Ensuring that repeated occurrence and use of infringing domain names does not take place.

On all these aspects, the stand of the Registry Operators and the DNRs has been non-cooperative to say the least. They either wish to take shelter under agreements entered with ICANN or seek safe-harbour protection under Section 69A of the IT Act.

219. The extensive submissions made and the documents placed before this Court leave no manner of doubt that the DNRs and Registry Operators earn a substantial amount of revenues by offering domain names registrations consisting of well-known marks, famous brands, and corporate house names. Various modes in which such revenues are earned are set out below:

(i) By offering domain names with varying extensions/suffixes of well-known brands, marks on premium rates.

(ii) By offering certain domain names categorised as 'premium' which are sold at exorbitant prices.

(iii) Some Registry Operators offer services of blocking of domain names as premium services for which payments would have to be made by the respective IP owners.

(iv) By offering marketing and Search Engine Optimization services to promote websites/domain names including even illegal and fraudulent websites/domain names consisting of third-party mark.

(v) By putting infringing domain names in the common pool so that revenues can be earned repeatedly, though said domain names have been declared to be infringing.

(vi) By adopting discriminatory practices in respect of entities and marks with whom they have special arrangements.

(vii) By offering after market services in domain name

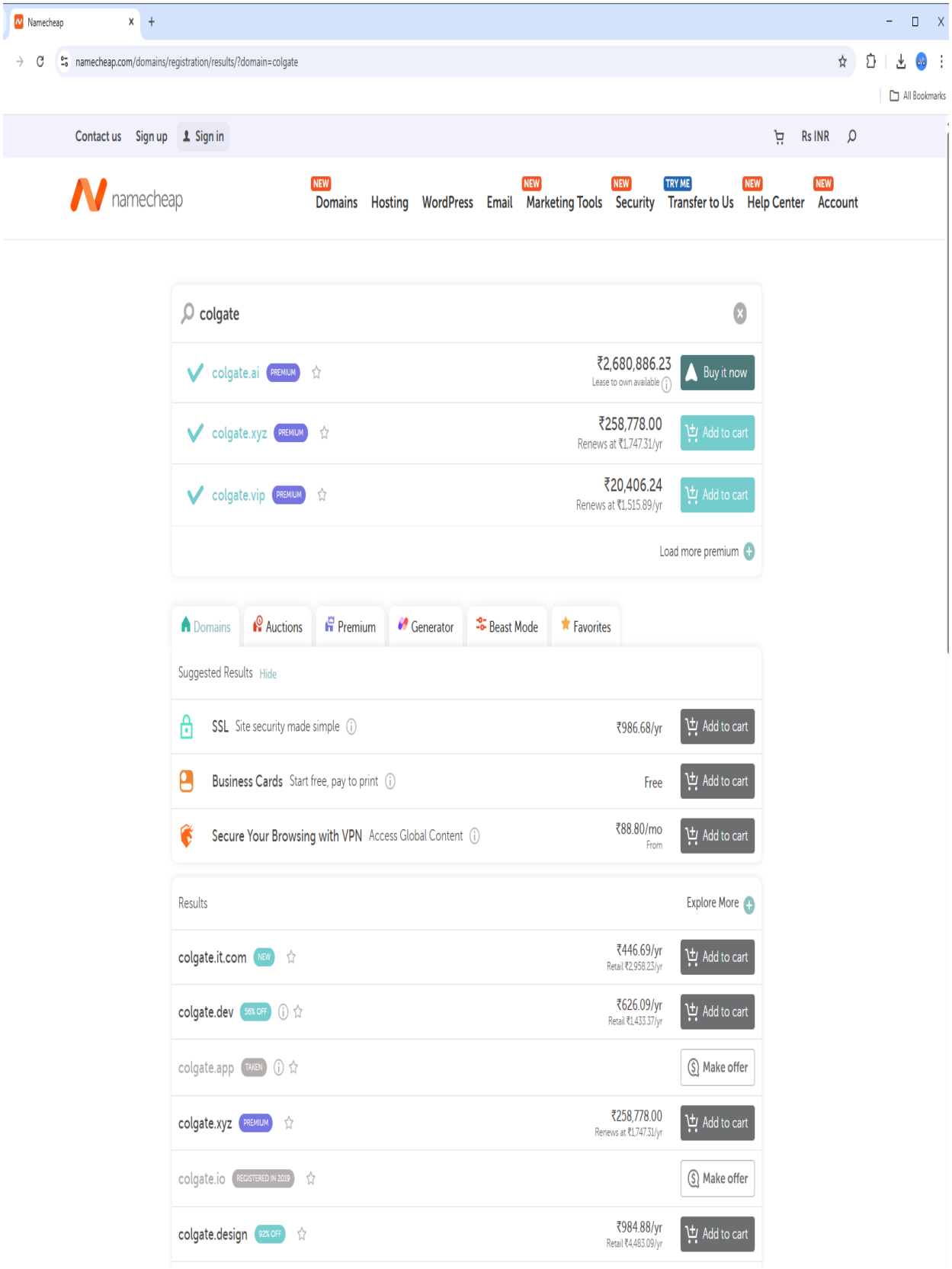
(viii) By operating domain name auction services whereby, the DNRs promote buying and selling of domain names as a way of investment. In effect this promotes monetising of the domain names even where the same violates the rights of third parties.

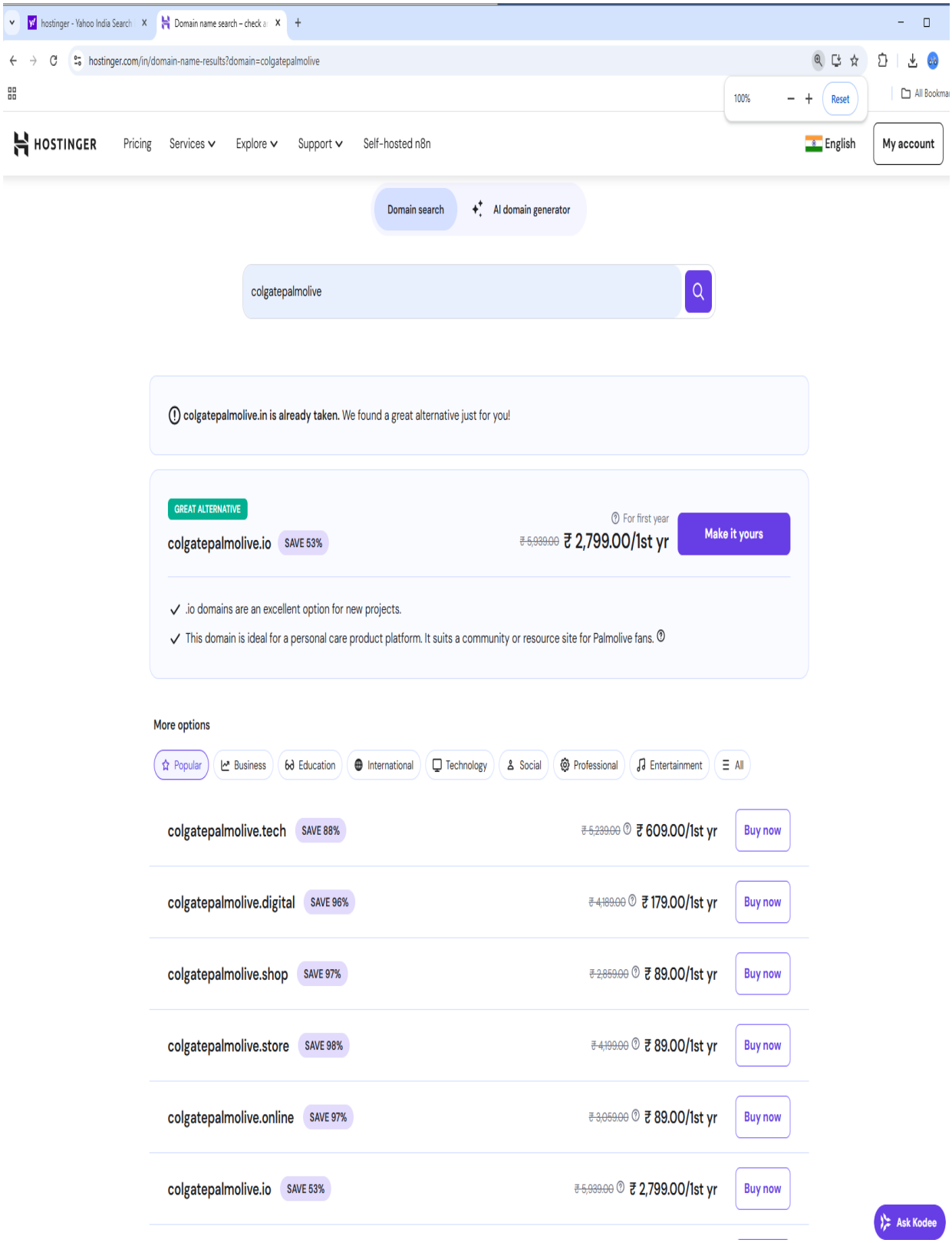
(ix) By providing brokerage services for assisting a new Registrant wishing to obtain an already registered domain name, purchase the same and transfer it to the new Registrant.

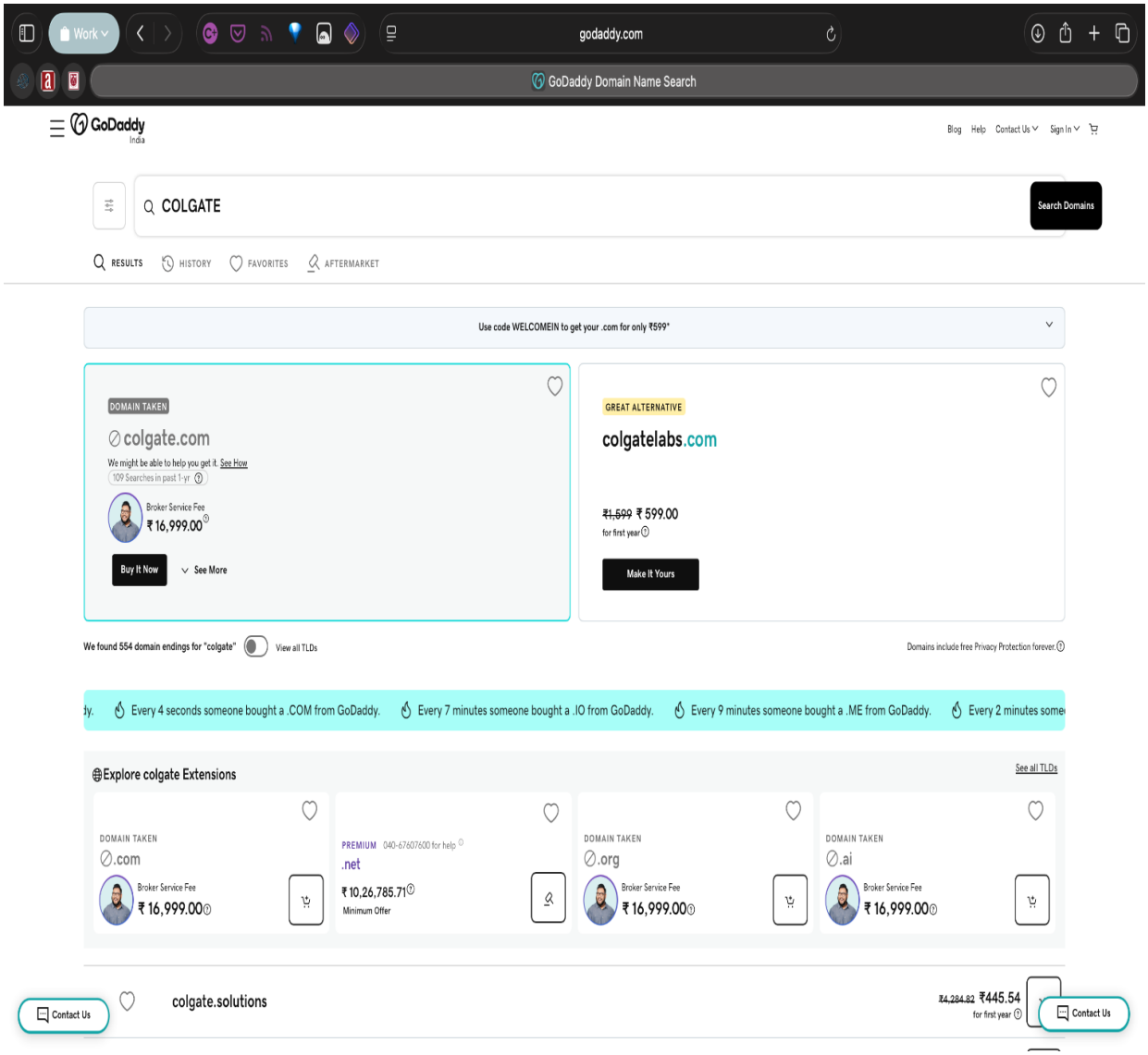
(x) A number of the DNRs also provide webhosting, marketing, and other support services to infringing domain names, thereby garnering substantive revenues. However, these facts are not usually disclosed to the Court.

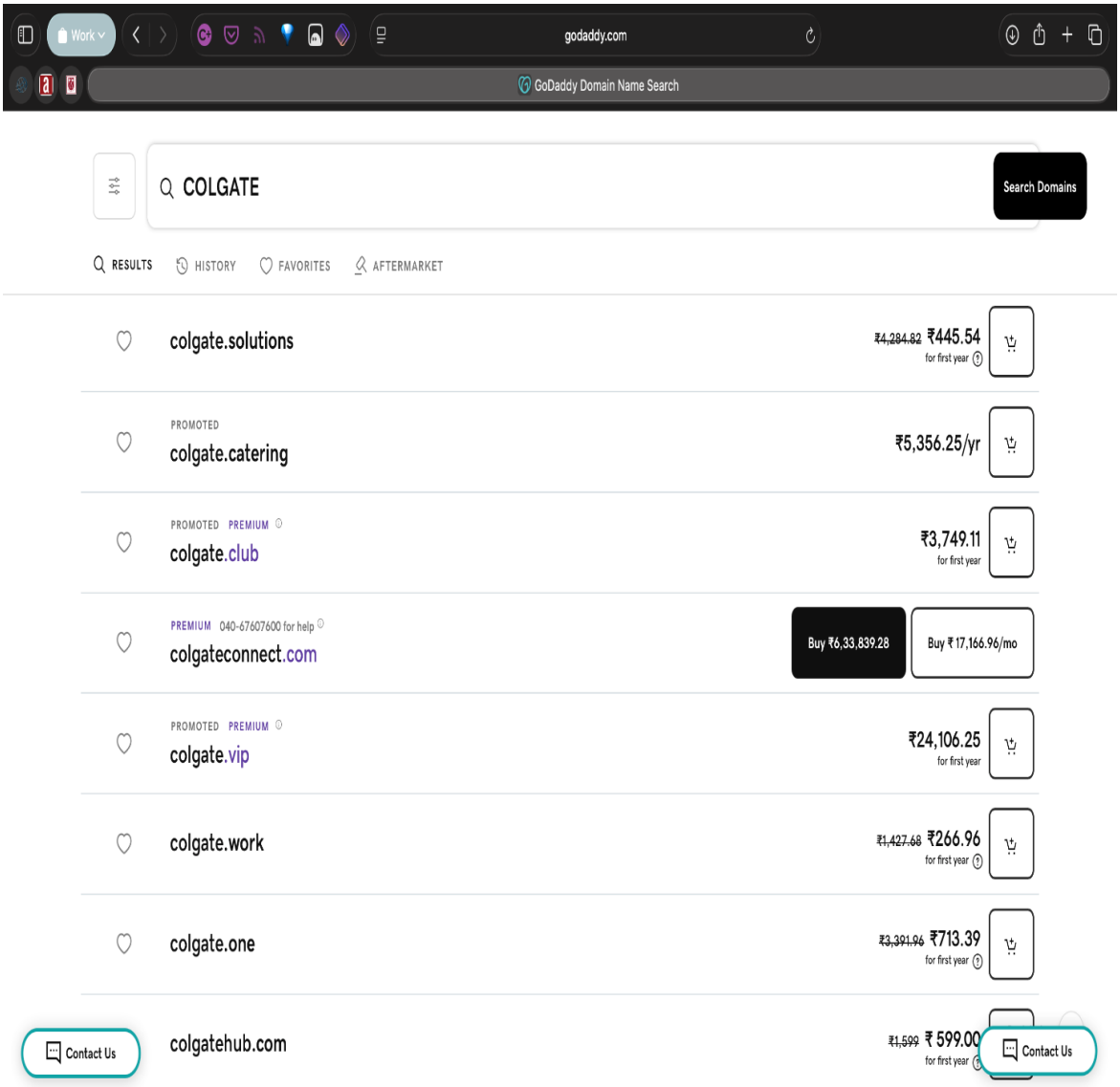
(xi) By not implementing technologies, which are available with them for ensuring that well known marks and registered trade marks are not misused to prevent cyber fraud, only with a view to maximise revenues.

220. In order to illustrate the above points as also to highlight the blatant disregard for the rights of trademark owners, certain screenshots taken from the websites of few DNRs are reproduced hereunder,:


Namecheap
namecheap.com/domains/registration/results/?domain=colgate
All Bookmarks
Contact us
Sign up
Sign in
Rs INR
namecheap
Domains
Hosting
WordPress
Email
Marketing Tools
Security
Transfer to Us
Help Center
Account
colgate
colgate.ai PREMIUM ₹2,680,886.23 Lease to own available Buy it now
colgate.xyz PREMIUM ₹258,778.00 Renews at ₹1,747.31/yr Add to cart
colgate.vip PREMIUM ₹20,406.24 Renews at ₹1,515.89/yr Add to cart
Load more premium
Domains
Auctions
Premium
Generator
Beast Mode
Favorites
Suggested Results Hide
SSL Site security made simple ₹986.68/yr Add to cart
Business Cards Start free, pay to print Free Add to cart
Secure Your Browsing with VPN Access Global Content ₹88.80/mo From Add to cart
Results
Explore More
colgate.it.com NEW ₹446.69/yr Retail ₹2,958.23/yr Add to cart
colgate.dev 56% OFF ₹626.09/yr Retail ₹1,433.37/yr Add to cart
colgate.app TAKEN Make offer
colgate.xyz PREMIUM ₹258,778.00 Renews at ₹1,747.31/yr Add to cart
colgate.io REGISTERED IN 2019 Make offer
colgate.design 92% OFF ₹984.88/yr Retail ₹4,483.09/yr Add to cart


hostinger - Yahoo India Search
Domain name search – check
hostinger.com/in/domain-name-results?domain=colgatepalmolive
HOSTINGER
Pricing
Services
Explore
Support
Self-hosted n8n
English
My account
Domain search
AI domain generator
colgatepalmolive
colgatepalmolive.in is already taken. We found a great alternative just for you!
GREAT ALTERNATIVE
colgatepalmolive.io
SAVE 53%
For first year
₹ 5,999.00 ₹ 2,799.00/1st yr
Make it yours
.io domains are an excellent option for new projects.
This domain is ideal for a personal care product platform. It suits a community or resource site for Palmolive fans.
More options
Popular
Business
Education
International
Technology
Social
Professional
Entertainment
All
colgatepalmolive.tech SAVE 88% ₹ 5,239.00 ₹ 609.00/1st yr Buy now
colgatepalmolive.digital SAVE 96% ₹ 4,199.00 ₹ 179.00/1st yr Buy now
colgatepalmolive.shop SAVE 97% ₹ 2,859.00 ₹ 89.00/1st yr Buy now
colgatepalmolive.store SAVE 98% ₹ 4,199.00 ₹ 89.00/1st yr Buy now
colgatepalmolive.online SAVE 97% ₹ 3,059.00 ₹ 89.00/1st yr Buy now
colgatepalmolive.io SAVE 53% ₹ 5,999.00 ₹ 2,799.00/1st yr Buy now
Ask Kodee

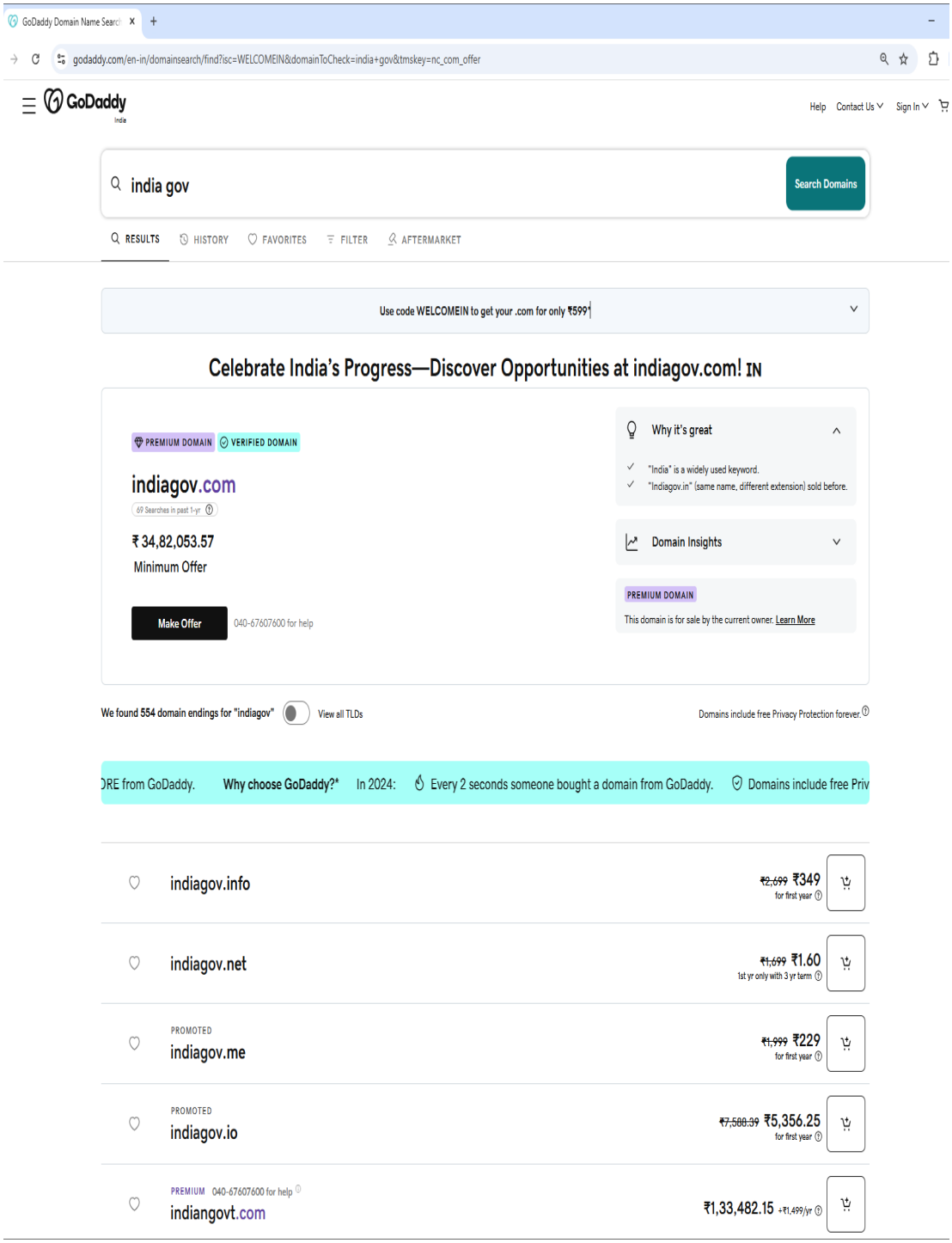

godaddy.com
GoDaddy Domain Name Search
GoDaddy India
Blog Help Contact Us Sign In
COLGATE
Search Domains
RESULTS HISTORY FAVORITES AFTERMARKET
Use code WELCOMEIN to get your .com for only ₹599*
DOMAIN TAKEN
colgate.com
We might be able to help you get it. See How
109 Searches in past 1-yr
Broker Service Fee
₹ 16,999.00
Buy It Now
See More
GREAT ALTERNATIVE
colgatelabs.com
₹1,599 ₹ 599.00
for first year
Make It Yours
We found 554 domain endings for "colgate"
View all TLDs
Domains include free Privacy Protection forever.
Every 4 seconds someone bought a .COM from GoDaddy.
Every 7 minutes someone bought a .IO from GoDaddy.
Every 9 minutes someone bought a .ME from GoDaddy.
Every 2 minutes some
Explore colgate Extensions
See all TLDs
DOMAIN TAKEN
.com
Broker Service Fee
₹ 16,999.00
PREMIUM 040-67607600 for help
.net
₹ 10,26,785.71
Minimum Offer
DOMAIN TAKEN
.org
Broker Service Fee
₹ 16,999.00
DOMAIN TAKEN
.ai
Broker Service Fee
₹ 16,999.00
Contact Us
colgate.solutions
₹4,284.82 ₹445.54
for first year
Contact Us



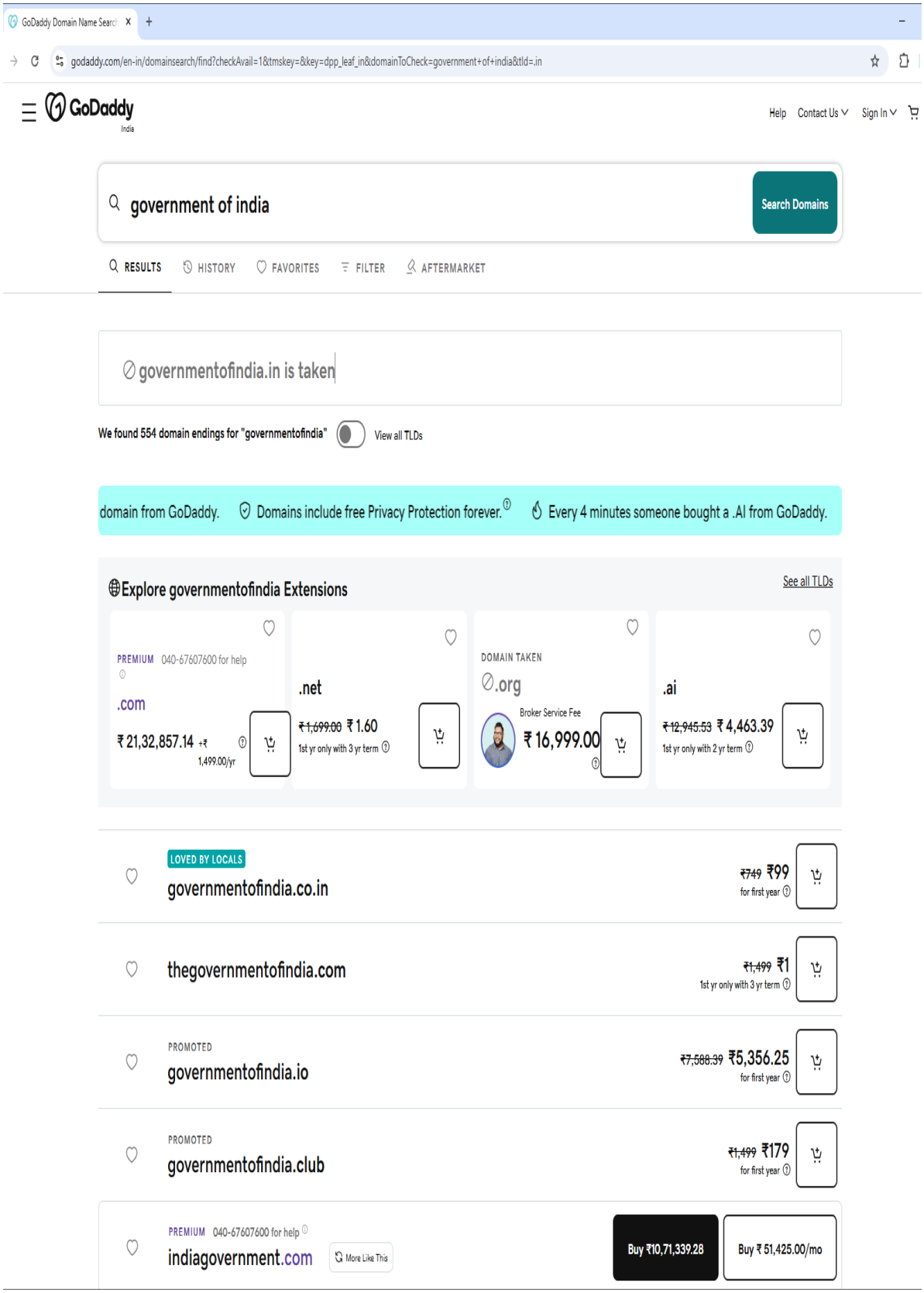
221. It is evident from the above screenshots that the DNRs are not only actively promoting alternative infringing domain names, with different prefix and suffix or different TLD, the DNRs are also consciously charging exorbitant prices for certain domain names that are most likely to infringe the marks of third parties.

222. However, apart from violation of private rights of the third parties, there is a greater concern which needs to be addressed and has been brought to the attention of this Court *i.e.,* when the infringing domain names of the private entities are so readily promoted and utilised for committing fraud, then shouldn't the mere possibility of an unscrupulous Registrant operating a domain name of the government or its instrumentalities demand overhauling of the present system? In order to fully appreciate the same, the Court, in the course of writing the judgement has researched similar domain names being made available of the following public entities:

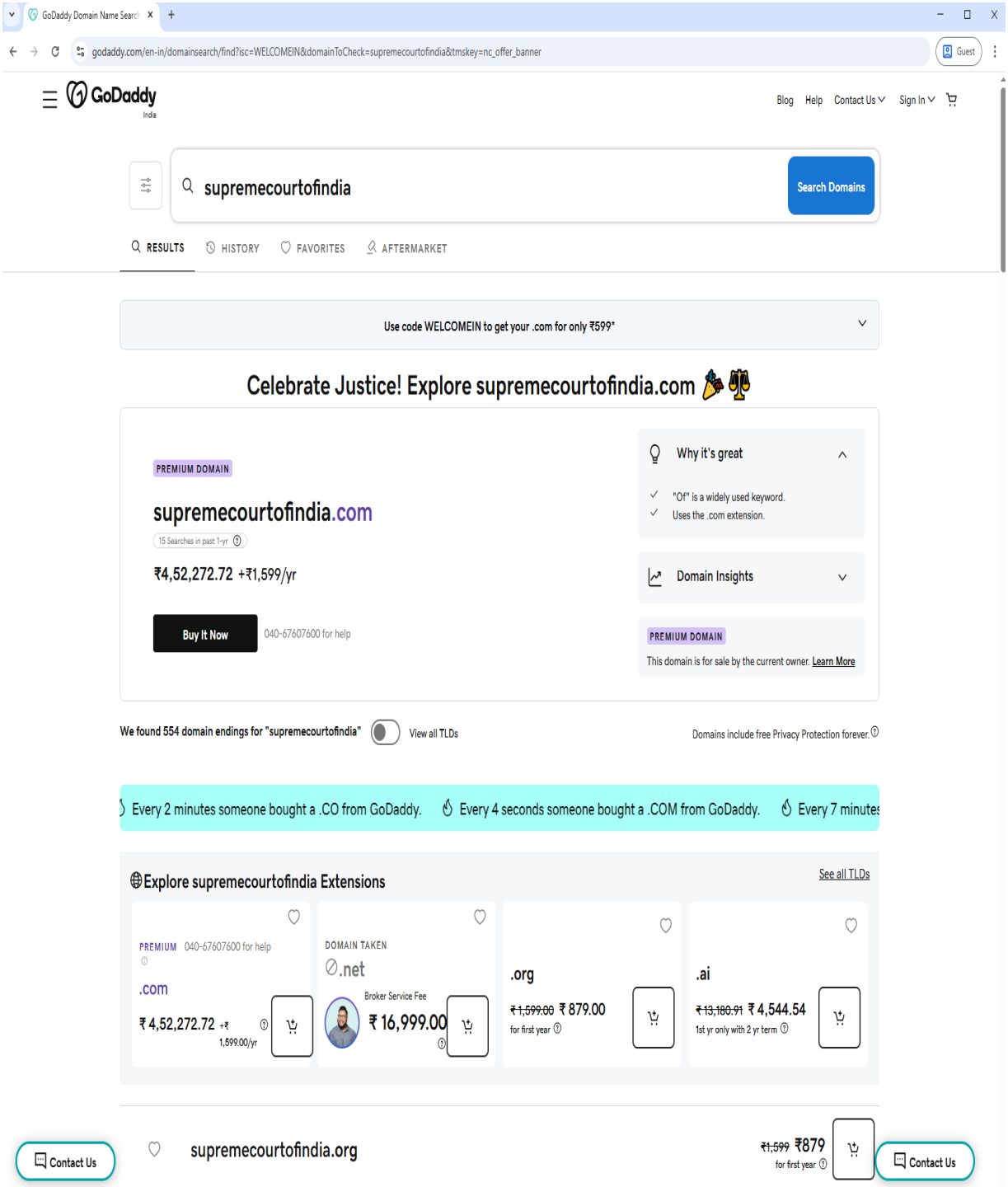
(i) Government of India (Actual domain name: https://india.gov.in/)

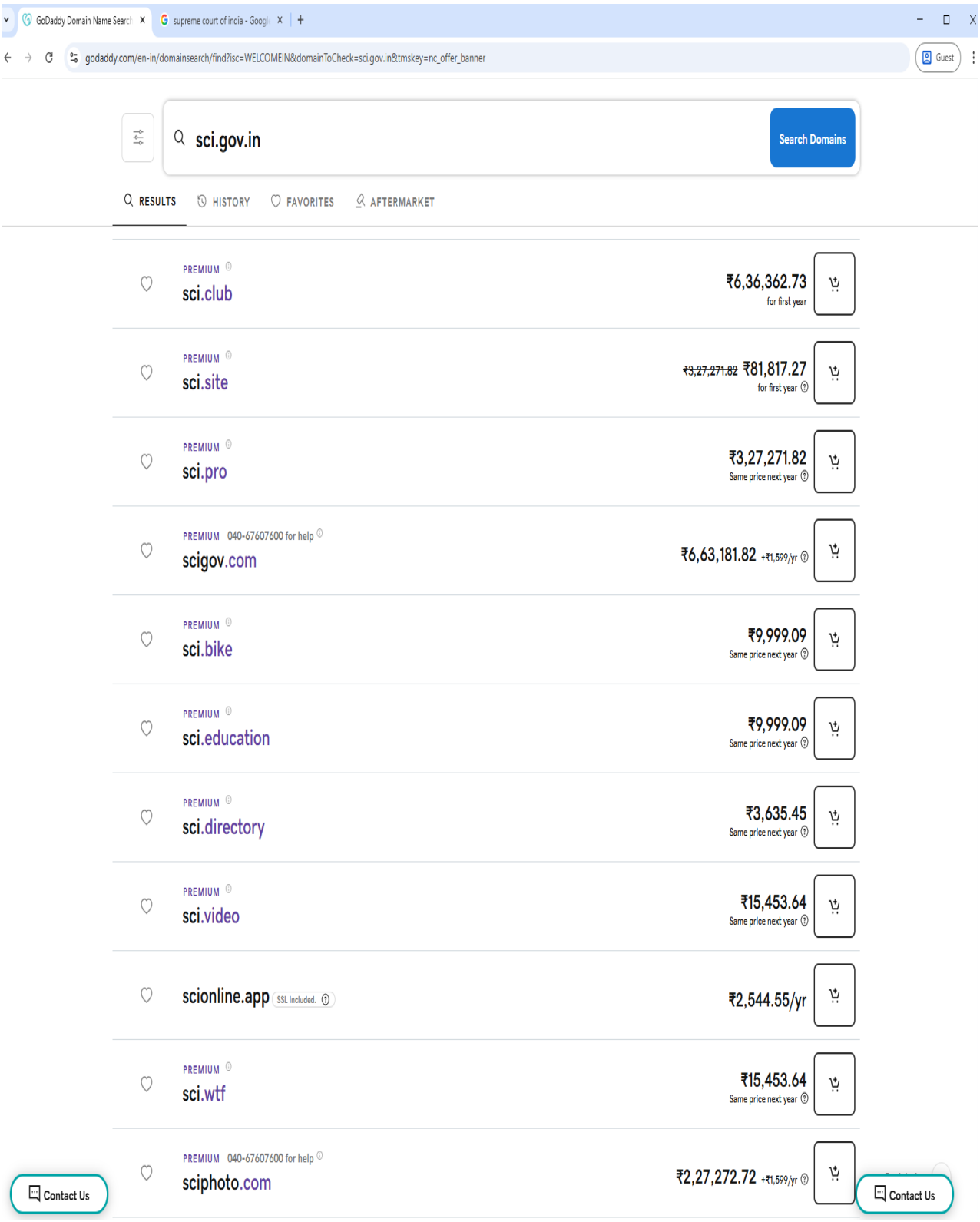


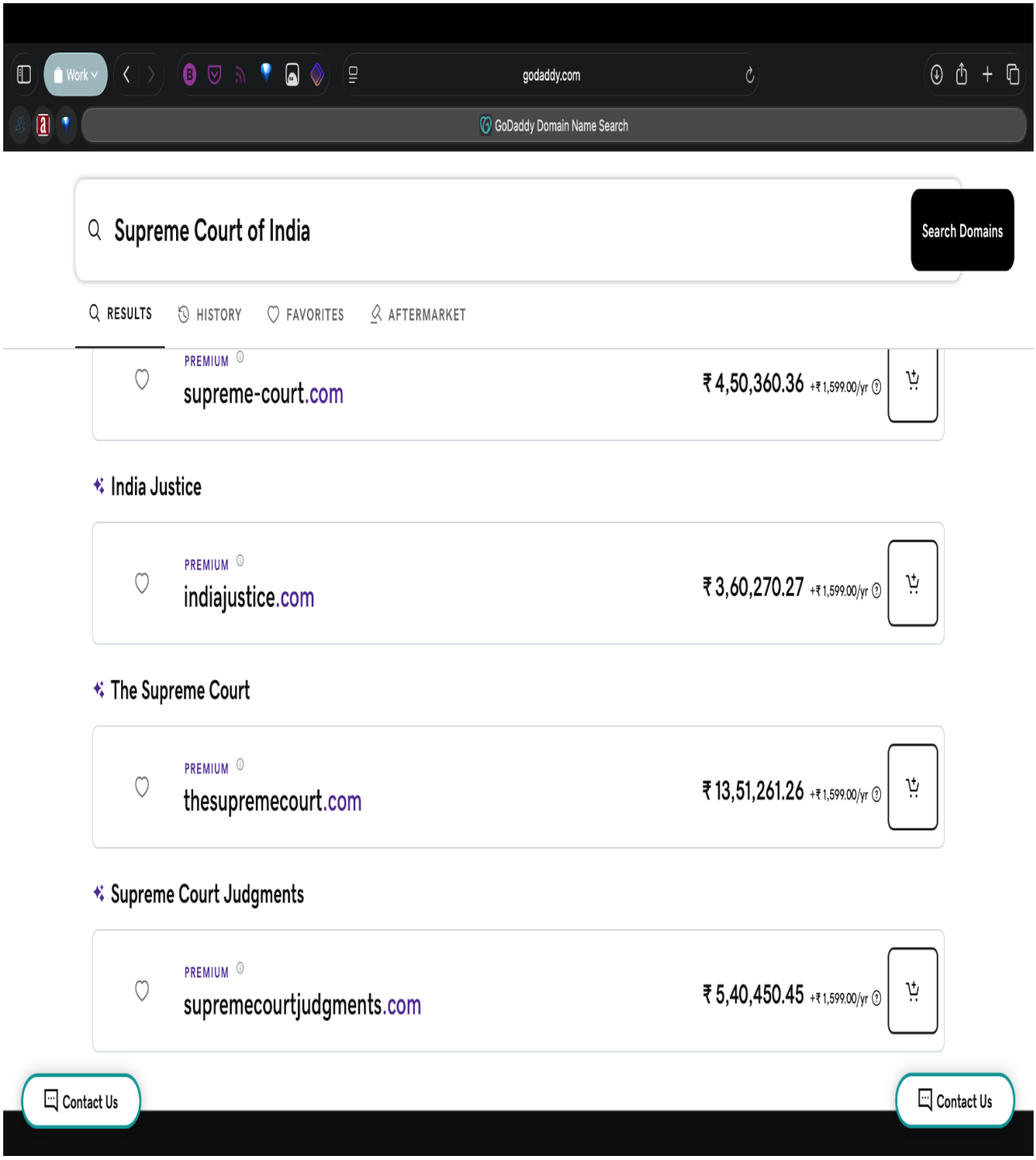
2025:DHC:11874



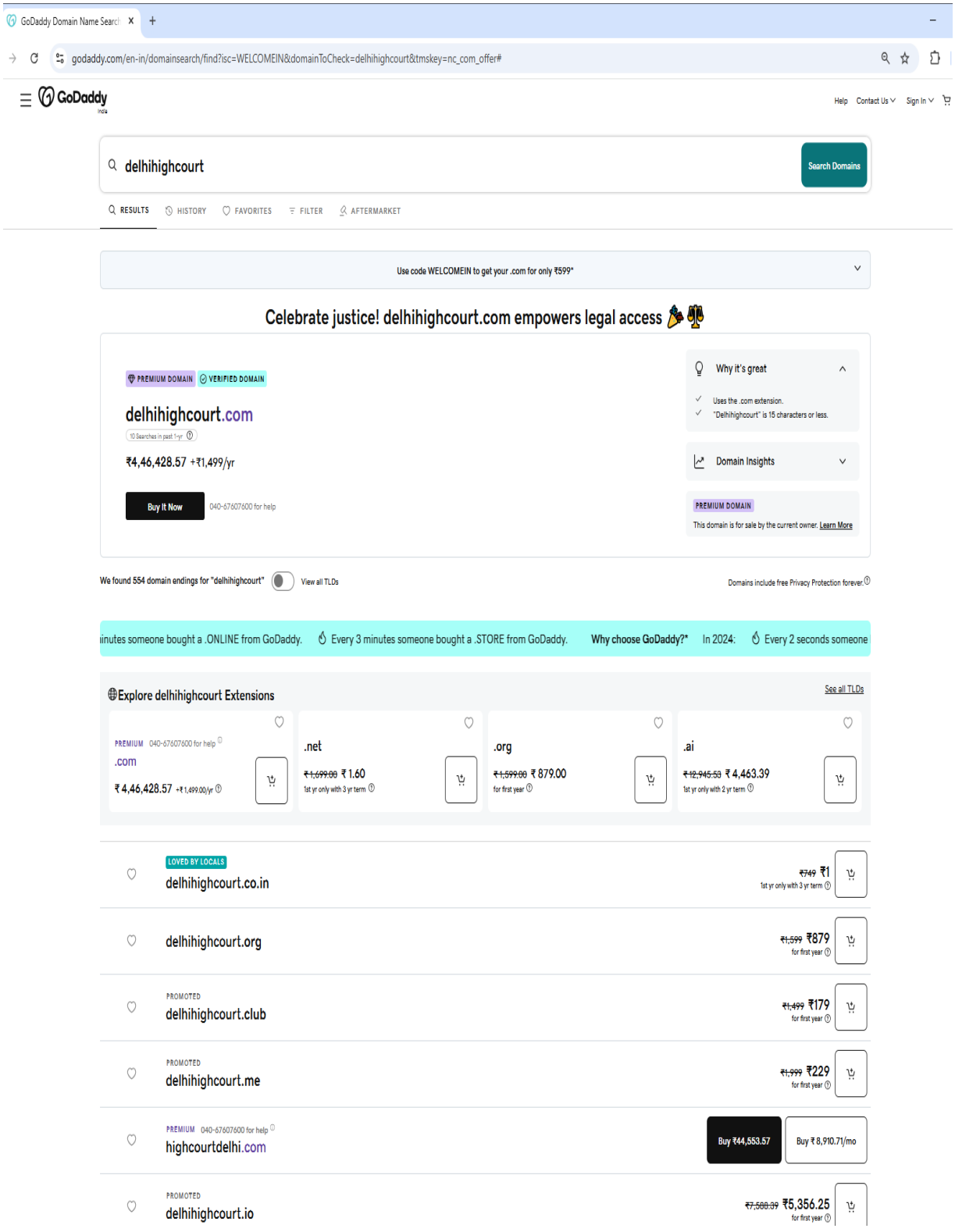
(ii) Supreme Court of India (Actual domain name: https://www.sci.gov.in/)



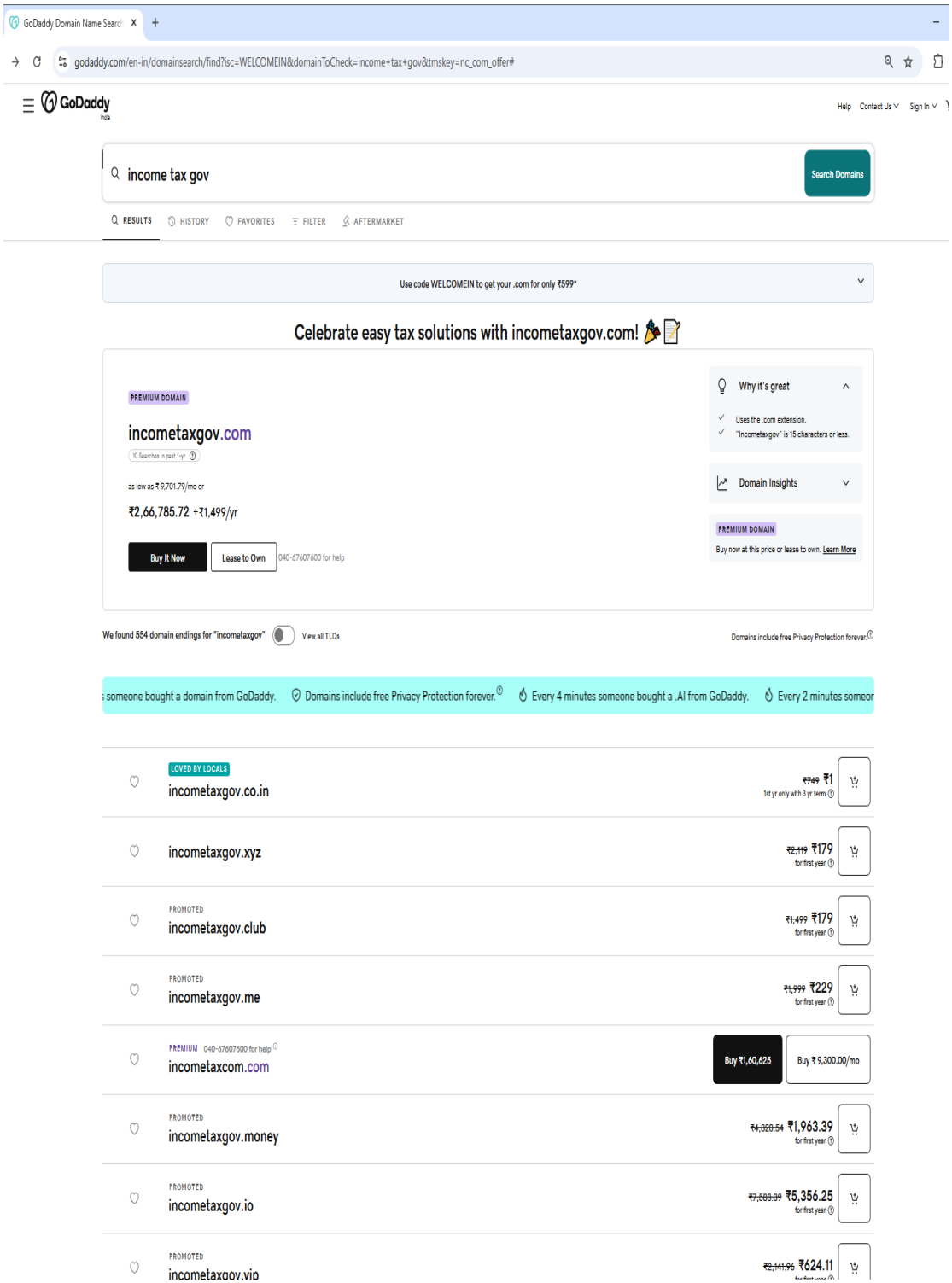

GoDaddy Domain Name Search
supreme court of india - Google Search
godaddy.com/en-in/domainsearch/find?isc=WELCOMEIN&domainToCheck=sci.gov.in&tmskey=nc_offer_banner
Guest
sci.gov.in
Search Domains
RESULTS
HISTORY
FAVORITES
AFTERMARKET
PREMIUM sci.club ₹6,36,362.73 for first year
PREMIUM sci.site ₹3,27,271.82 ₹81,817.27 for first year
PREMIUM sci.pro ₹3,27,271.82 Same price next year
PREMIUM 040-67607600 for help scigov.com ₹6,63,181.82 +₹1,599/yr
PREMIUM sci.bike ₹9,999.09 Same price next year
PREMIUM sci.education ₹9,999.09 Same price next year
PREMIUM sci.directory ₹3,635.45 Same price next year
PREMIUM sci.video ₹15,453.64 Same price next year
scionline.app SSL Included. ₹2,544.55/yr
PREMIUM sci.wtf ₹15,453.64 Same price next year
PREMIUM 040-67607600 for help sciphoto.com ₹2,27,272.72 +₹1,599/yr
Contact Us
Contact Us


Work
godaddy.com
GoDaddy Domain Name Search
Supreme Court of India
Search Domains
RESULTS
HISTORY
FAVORITES
AFTERMARKET
PREMIUM
supreme-court.com
₹ 4,50,360.36 +₹ 1,599.00/yr
India Justice
PREMIUM
indiajustice.com
₹ 3,60,270.27 +₹ 1,599.00/yr
The Supreme Court
PREMIUM
thesupremecourt.com
₹ 13,51,261.26 +₹ 1,599.00/yr
Supreme Court Judgments
PREMIUM
supremecourtjudgments.com
₹ 5,40,450.45 +₹ 1,599.00/yr
Contact Us
Contact Us

(iii) Delhi High Court (Actual domain name: https://delhihighcourt.nic.in/)



(iv) Income Tax Department, Govt. of India (Actual domain name: https://www.incometax.gov.in/)



The above illustrative screenshots from GoDaddy's website would show how easy it is for scamsters and unscrupulous persons to pay and obtain these domain names and also utilise the same, to engage in cyberfraud. Recent instances of digital extortion is made possible without much effort due to illegal registration of such websites/domain names. Providing domain names such as Government of India, Supreme Court of India, Delhi High Court, Income Tax Department is not merely violative of IP rights but in effect an encouragement for indulging in unlawful activity. Such acts of DNRs would also impinge upon the sovereignty and integrity of the country.

223. It is evident from the above that there is a clear and pressing need for establishing certain safeguards in the present system of domain name registration. In the absence of the same, DNRs shall continue to generate profits from selling domain names which may result in widespread injury to the public at large. The Court need not labour upon the possibilities of the harm that may be caused if an unscrupulous individual register the domain names as shown above and creates an unsurmountable trust deficit between the public authorities and the public at large by defrauding them in the name of said authorities.

224. It is noticed by the Court that the DNRs and Registry Operators have the technology to lock, block, suspend and deactivate the infringing domain names and ensuring that the same domain names do not resolve into a website. However, as seen in the present batch matters, these services are not being implemented despite frantic requests even from LEAs and trademark owners. Most DNRs take shelter under the different laws such as GDPR to give a cloak and camouflage to the illegal usurpers of the trademark and brand names.

Further, although almost all the DNRs obtain payments for these infringing domain names through electronic transactions, but the details of the persons making the payment for registering the domain names are not furnished in time by the DNRs.

225. The only genuine detail that is obtained from the DNRs and Registry Operators is the email address and nothing more, the correctness of which is also not guaranteed. No mobile number, Aadhar card, any government identity card, passport details or any such verifiable detail is obtained, which is made available to the Court or to the person with legitimate interest, to enable proper enforcement of rights of the IP owners and prevention of cyber frauds. This is despite the fact that the relevant agreements of DNRs with ICANN itself stipulate that the contact details have to be collected and verified periodically.

226. Crores of rupees are collected through bank accounts and electronic payments by these unscrupulous websites and domain names holders. However, the IP owners are unable to recover any damages, and neither are the members of the public being returned the amounts innocently deposited by them, due to the repeated road blocks and obstacles created by the DNRs. The DNRs and Registry Operators possess sufficient technological means to block, lock, or suspend the illegal and infringing domain names from being registered. However, grant of such reliefs is opposed on the ground that the same would be violative of the right to free speech and affect the rights of some legitimate owners who may wish to register the said domain names.

227. One of the most important aspects in all these commercial suits, which involve about 1132 infringing domain names as on date, is that, barring one or

two domain names, no *bona fide* Registrant has come forward claiming any legitimate right to use the infringing domain names. None of the Registrants have participated in the present proceedings which have been ongoing since 2022, despite the fact that respect of most domain names, an order of injunction is operating. Almost all the Registrants of infringing domain names are fly-by-night operators, operating the websites with or without any physical premises, who fraudulently collected moneys by using marks and the names of the Plaintiffs. These Registrants have completely vanished into thin air once the money is collected. Even before the brand owner realizes about the collection of money by unscrupulous individuals and the entities, the collected money is transferred or withdrawn without a trace. In some of the suits, the police have also arrested some individuals but there is still no trace of the money. By way of an illustration, a table is set out below giving the details of the amounts, which have been collected in some of the commercial suits:

Sr. No.	Case Details	Amounts Debited	FIR Details
1.	Hindustan Unilever Ltd. v. Nitin Kumar Singh & Ors. CS(COMM) 399/2021	Rs. 6,05,000/-	FIR No. 262/2021, P.S. Special Cell, U/S 420/468/471 of IPC
2.	Hindustan Unilever Ltd. & Anr. v. Unilever1.in & Ors. CS(COMM) 275/2022	Rs. 4,34,700/-	FIR No. 219/22 U/s 419/420 IPC & Sec. 66C/66D of IT Act; FIR No. 6/2022 P.S. Cyber Cell.
3.	Gujarat Cooperative Milk	Rs. 6,50,000/-	FIR No. 226/2022

	Marketing Federation Ltd. & Anr. v. Amul Franchise.in & Ors. CS(COMM) 350/2020		U/S 419/420 of IPC & Sec. 66C/66D of IT Act.
4.	Bajaj Finance Ltd. & Anr. v. Niko Das & Anr. CS(COMM) 233/2022	Rs. 22,71,909/-	FIR No. 215/2022 U/S 419/420 & Sec. 66C/66D of IT Act.
5.	ITC Limited v. Ashok Kumar & Ors. CS(COMM) 373/2020	Rs. 37,73,674/-	Investigation ongoing.
6.	Montblanc Simplo GMBH v. Montblacindia.com & Ors.	Rs. 11,03,85,196/-	Investigation ongoing.
7.	Indiamart Intermesh Ltd. v. Sameer Samim Khan & Ors. CS(COMM) 631/2022	Rs. 10,00,000/- (approx.)	FIR No. 296/2022 U/S 419/468/471 & Sec. 66C/66D of IT Act, P.S. Special Cell
8.	Burger King Corp. v. Swapnil Patil & Ors. CS(COMM) 303/2022	Rs. 87,000/-	-

228. The genesis of this kind of large scale fraudulent and illegal activity, which is taking place, is registration of the domain names, which consists of the trademarks, brands names and well known business and corporate house such as Dabur, Tata, Colgate, Amazon, Hindustan Unilever, Microsoft, Bajaj etc. Courts cannot be powerless in such a situation and this malady needs to be nipped in the bud. For the said purpose, whatever measures are required to be taken in accordance with law ought to be directed as the Court is not merely safeguarding the interest of the Plaintiffs, who are the IP owners but has a larger duty to the

general public to ensure that the misuse of these domain names for offering of jobs, dealerships, franchises and collecting monies under the garb of such offers is eliminated as much as possible. Further, the sale of counterfeit products by registering the domain names with highly reputed global brands such as Montblanc also deserves to be restrained.

229. The privacy protection features adopted by DNRs, which is a trend that has been observed over the last few years, also has a major role to play in promoting camouflage registration of the domain name and making it an extremely challenging process to obtain the details of the Registrants. It is observed that when the whole system of domain name registration had started sometime in late 1990s and early 2000s, the WHOIS data base would reveal the details of the Registrants of the domain names upon a simple search. However, over the years privacy protection has been implemented as default mode by most of the DNRs. Further it is also seen that in several cases these infringing domain names may have been registered by the affiliates and group companies of the DNRs itself. The non-disclosure of details gives a head-start to the Registrant of the illegal and infringing domain names as the process of obtaining the data relating to a Registrant is time consuming and difficult. This is despite the fact that any person, who has a legitimate interest in a domain name or mark ought to be permitted to have the details simply by writing an email to the DNR. Even when such an email is written, full disclosure is not made by the concerned DNR resulting in lengthy correspondence between the trademark owners and the DNR concerned. In the course of these hearings, several such emails have been noticed by the Court where obtaining of registrant details from the DNRs has proved to

be a cumbersome process.

230. The attempt of a right holder to obtain details of a Registrant is further made difficult due to the fact that the said Registrant may have utilised the services of a proxy because of which the details of the said proxy would be shown in place of the details of the Registrant. These privacy protect and proxy services, which are provided as valued added services, have been made as default services for almost all domain name registrations by the DNRs. Whereas in comparison, NIXI in its agreement for accreditation of DNRs has prohibited the use of privacy protect and proxy services. Further, the use of temporary email addresses has been specifically denied. The terms and conditions prescribed by NIXI for all Registrants utilising '.in' domain names, expressly mentions this position.

Measures implemented by DNRs and Registry Operators:

231. At this stage it would also be relevant to consider the submissions of the DNRs and Registry Operators as to what measures they are willing to take against an infringing domain name. On behalf of two DNRs - GoDaddy and Newfold Digital Inc., it was submitted that actions which they can take pursuant to a Court order is as follows:

(i) Suspend the domain name for duration of its registration.

(ii) Lock the domain name for transfer of the domain name for the duration of its registration. Cost would have to be borne by the rights holder for implementing any measure beyond the period of registration of the domain name.

(iii) Disclose the Registrant data and payment details as available with the DNR.

(iv) Transfer the domain name to the rights holder subject to payment of the applicable costs.

The said DNRs have also submitted that after the order of the Court in respect of the infringing domain names is passed, the subsequent orders can be passed by the Joint Registrar upon appropriate applications with affidavits being filed by the rights holder.

232. However, the said DNRs have also argued as to what measures they cannot or are unwilling to take against the infringing domain names, which are as follows:

(i) They cannot block, block access, take down, delete or remove domain names.

(ii) They cannot suspend the domain name permanently.

(iii) They cannot take any steps against the website, URLs, sub-domain or webpages. These are under the domain of web hosting service providers or the Internet Service Provider.

(iv) They cannot disclose payment details which are not on their record.

(v) They cannot block specific word strings or suspend all domain names which contain the specific domain names. It is argued that the same ought to be done by the Registry Operators for the specific TLD.

233. In ***Hindustan Uniliver Limited v. Endurance Domains Technology LLP & Ors., 2020 SCC OnLine Bom 809,*** the ld. Single Judge of the Bombay High Court has highlighted the fact that DNRs can only suspend the domain name registration and cannot block the website. The difficulty that arises is, even if a domain name is suspended and the website may not become accessible, after the

registration of the domain name expires, it falls into the public domain and thereafter be renewed by third party. Mere suspension may not be enough and certain other measures would also have to be taken in this regard.

234. Further, the stand of Hosting Concepts – another DNR, in fact, shows that Registry Operators have the capability to implement Court orders that may be passed much beyond the identified infringing domain names, by implementing services/features such as Trademark Clearing House, Domain Protected Marks List and Adult Block. This should be read along with the submissions on behalf of Registry Operator Verisign, which stated that in order to comply with the directions of the Court for blocking, locking or suspending the infringing domain names the Registry Operators may implement EPP status codes such as *serverHold, serverRenewProhibited, serverDeleteProhibited* etc.

235. There is also the possibility of adding certain strings of words in Reserved Lists maintained by the Registry Operators, which would prevent these from being available for registration. Moreover, NIXI in its response to Meity, has stated that "*Nixi is fully equipped to be a data repository agency provided due acceptance is received from competent authority. NIXI is a data Centre business thereby secure storage of WHOIS details is ensured*".

236. Thus, there are several measures which the DNRs and Registry Operators may take for ensuring that the infringing domain name is no longer accessible to the general public or is added in the common pool for being utilised again, by transferring the same to the respective mark holder. However, despite the possible measures which may be implemented against infringing domain names, the same would be rendered toothless if the concerned DNRs and Registry

Operators do not comply with the orders of the Court.

ISSUE III: WHAT MEASURES MAY BE DIRECTED BY THE COURT AGAINST DNRS WHO REFUSE TO COMPLY WITH THE COURT ORDERS?

Intermediary obligations of due diligence and safe harbour protection

237. One of the issues that has been raised is whether if the DNR does not comply with the order passed by a Court, what would be the method of enforcing the said order. This Court has come across several instances in the present batch of suits where the Registry Operators and DNRs have taken extremely unreasonable stance of asking the persons with legitimate interest in India to obtain a subpoena or an order from the Court of a foreign jurisdiction, such as Courts in United States of America, for enforcing orders passed by Indian Courts. It is routinely observed that the orders of Indian Courts are not being given effect to in a timely manner, especially by those DNRs and Registry Operators operating from foreign shores. Some Registry Operators and DNRs insist on service through international institutions such as Hague Convention and MLAT even when there is an immediate threat to the interest of innocent members of the public. This position led the Court to issuing orders directing the services of the non-compliant DNRs to be blocked by the concerned authority. It was only pursuant to such directions that the non-compliant DNRs took steps to comply with the orders of the Court.

238. However, on this aspect, there is a considerable divergence in opinion between the Plaintiffs and the Defendants *i.e.,* the DNRs, as no valid Registrant

of a domain name has set up any defence in these cases. The Plaintiffs pray that such DNRs, who are not implementing the orders passed by the Indian Courts, ought not to be allowed to conduct business in India and their services themselves should be blocked in terms of Section 69A of the IT Act, as the same would impinge upon the sovereignty of the Court and hence the country, create disturbance in public order and also incite commission of cognizable offences. On the other hand, the DNRs argue that such extreme steps ought not to be resorted to. The DNRs and Registry Operators claim to be intermediaries and hence invoke the protection of safe harbour under Section 79 of the IT Act. Further reliance is placed on the submission on behalf of the Government by MeitY, wherein it was stated that in some cases other innocent registrants of domain names registered by the same DNR could be put to enormous inconvenience if such DNRs services are totally blocked.

239. Considering all these competing stands, there is a need to put in place a proper system, which shall be complied with by all the DNRs, especially when domain names, which are clearly infringing, have been registered. Moreover, the Plaintiffs, who are trademark owners, cannot also be expected to perpetually be in a state of litigation and continue to obtain injunctions from the Courts of law as the same involves substantial expenses.

240. At the outset, since, the DNRs and Registry Operators claim to be protected as intermediaries under Section 79 of the IT Act, and whereas the Plaintiff and Government support blocking of the non-compliant DNRs under Section 69A of the IT Act, it would be relevant to reproduce the said sections, along with Section 81 of the IT Act which grants overriding effect to the

provisions of IT Act. The said Sections read as under:

> *"**Section 69A. Power to issue directions for blocking for public access of any information through any computer resource**.–*
>
> *(1) **Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do**, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or **public order or for preventing incitement to the commission of any cognizable offence relating to above**, it may subject to the provisions of sub-section (2), **for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource**.*
>
> *(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.*
>
> *(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.*
>
> ***Section 79. Exemption from liability of intermediary in certain cases.–***
>
> *(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for*

any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if–

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not– (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission;

(c) ***the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf****.*

(3) ***The provisions of sub-section (1) shall not apply if****–*

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) ***upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner****.*

Explanation.–For the purposes of this section, the expression "third party information" means any

information dealt with by an intermediary in his capacity as an intermediary.

Section 81. Act to have overriding effect.–

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).”

241. Further, the Intermediary Rules, 2021 lay down what are the requirements of due diligence to be exercised by the intermediaries. The relevant portion of the said Rules reads as under:

“3. (1) Due diligence by an intermediary: An intermediary, including a social media intermediary, a significant social media intermediary and an online gaming intermediary, shall observe the following due diligence while discharging its duties, namely:—

(a) ***the intermediary shall prominently publish on its website, mobile based application*** *or both, as the case may be,* ***the rules and regulations, privacy policy and user agreement*** *in English or any language specified in the Eighth Schedule to the Constitution for access or usage of its computer resource by any person in the language of his choice and* ***ensure compliance of the same****;*

(b) the intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or

any language specified in the Eighth Schedule to the Constitution in the language of his choice and ***shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that****,—*

(i) belongs to another person and to which the user does not have any right; […]

(iv) ***infringes any patent, trademark, copyright or other proprietary rights****; […]*

(vi) impersonates another person;

(vii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation;
[…]

(d) an intermediary, on whose computer resource the information is stored, hosted or published, ***upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act****, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States;* ***public order****; decency or morality; in relation to contempt of court; defamation;* ***incitement to an offence relating to the above, or any information which is***

prohibited under any law for the time being in force*:*

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, ***the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be****:[...]*

(j) ***the intermediary shall, as soon as possible, but not later than seventy two hours*** *and in case of an online gaming intermediary who enables the users to access any permissible online real money game not later than twenty-four hours* ***of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative*** *or protective or cyber security activities,* ***for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force****, or for cyber security incidents:*

Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be;

[...]

*7. Non-observance of Rules.—****Where an intermediary fails***

> ***to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary*** *and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code."*

242. It would also be relevant to consider the relevant provisions of the Blocking Rules, 2009 which provide the procedure for blocking access to websites etc. The relevant provisions are extracted hereunder:

> ***"10. Process of order of court for blocking of information****.—In case of an order from a competent court in India for blocking of any information or part thereof generated, transmitted, received, stored or hosted in a computer resource, the Designated Officer shall, immediately on receipt of certified copy of the court order, submit it to the Secretary, Department of Information Technology and initiate action as directed by the court."*

243. The DNRs and Registry Operators have relied upon the decision in ***Shreya Singhal (supra)*** in support of their submissions that they are intermediaries and are only required to act upon receiving "actual knowledge" by way of an order of the Court of law or notification from governmental agencies. It is further argued that the DNRs and Registry Operators are complying with the due diligence requirements prescribed under the Intermediary Rules, 2021 through its Domain Name Registration Agreement for Registrants and through its grievance redressal mechanisms. It is also submitted that safe harbour protection granted to intermediaries cannot be diluted merely on the ground that value-added services are being offered by the intermediaries.

244. The issue in respect of the scope of safe harbour protection of intermediaries *vis-à-vis* the infringement or violation of IP rights of a party has been extensively considered by the Courts. In ***Christian Louboutin SAS vs. Nakul Bajaj & Ors., 2018:DHC:7106*** (decided on 2nd November, 2018) this Court was considering the said issue in respect of an e-commerce platform alleged to have infringed the trademark of the Plaintiff therein. The Court having considered the jurisprudence in different jurisdictions as also Indian decisions, including ***Shreya Singhal (supra),*** in respect of safe harbour protections held as under:

> *"62.* ***While the so-called safe harbour provisions for intermediaries are meant for promoting genuine businesses which are inactive intermediaries, and not to harass intermediaries in any way, the obligation to observe due diligence, coupled with the intermediary guidelines which provides specifically that such due diligence also requires that the information which is hosted does not violate IP rights, shows that e-commerce platforms which actively conspire, abet or aide, or induce commission of unlawful acts on their website cannot go scot free****.*
>
> *63. The elements summarised above would be key to determining whether an online marketplace or an e-commerce website is conspiring, abetting, aiding or inducing and is thereby contributing to the sale of counterfeit products on its platform. When an e-commerce website is involved in or conducts its business in such a manner, which would see the presence of a large number of elements enumerated above, it could be said to cross the line from being an intermediary to an active participant. In such a case, the platform or online marketplace could be*

liable for infringement in view of its active participation. Needless to add, e-commerce websites and online marketplaces ought to operate with caution if they wish to enjoy the immunity provided to intermediaries. The question, however, would have to be determined after reviewing the practices of various websites under the facts and circumstances of a particular case.

64. ***So long as they are mere conduits or passive transmitters of the records or of the information, they continue to be intermediaries, but merely calling themselves as intermediaries does not qualify all e-commerce platforms or online market places as one****.*

[...]

71. They do not and cannot substitute themselves either for the provision in the IT Act i.e., Section 79 or nullify provisions in other applicable laws. These guidelines are framed under Section 79(2) and would not negate the stipulations in Section 79(3)(a). The guidelines would not offer protection to any `intermediary' that have `conspired', `abetted' or `aided' or `induced the commission' of an unlawful act. It cannot be argued that anyone who complies with the guidelines is automatically not conspiring, abetting, aiding or inducing commission of an unlawful act. Following the guidelines may in certain cases satisfy that the online market place is behaving as an intermediary but the same is not conclusive. What is lawful or unlawful depends on the specific statute being invoked and the Guidelines cannot be considered as being exhaustive in their manner of application to all statutes.

76. ***The overriding nature of the IT Act has application only if the provisions of the Trade Mark Act are***

inconsistent with the provisions of the IT Act. *The Intermediary Guidelines 2011 themselves require compliance with the TM Act by the persons to host, display or upload the products or services. The provisions of Section 29, Section 101 and Section 102 of the TM Act, are being looked at in order to interpret as to what constitutes 'conspiring, abetting, aiding or inducing' the commission of an unlawful act, in the context of trade mark rights.* ***The provisions of the TM Act are not in any manner inconsistent with the provisions of the IT Act. Hence Section 81 of the IT Act does not grant any immunity to intermediaries who may be in violation of the provisions of the TM Act.*** *While, use of a mark for any of the purposes elaborated above, in respect of genuine goods of the owner would not be infringement, the performance of any service as elaborated above, in respect of counterfeit goods or goods which are not genuine, could constitute infringement.*

[...]

81. The trademark owner loses its huge customer base especially in the case of luxury products. If the products turn out to be counterfeit or not up to the mark, then it is the trademark owner's brand equity which is diluted. The seller himself does not suffer. Such immunity is beyond what is contemplated to intermediaries under Section 79 of the IT Act. While Section 79 of the IT Act is to protect genuine intermediaries, it cannot be abused by extending such protection to those persons who are not intermediaries and are active participants in the unlawful act. Moreover, if the sellers themselves are located on foreign shores and the trade mark owner cannot exercise any remedy against the said seller who is selling counterfeits on the e-commerce platform, then the trade

mark owner cannot be left remediless."

245. The Court emphasised that safe-harbour under Section 79 of the IT Act is meant only for genuine, passive intermediaries, not for platforms that actively facilitate unlawful activity. Any intermediary would lose its safe harbour protection if found conspiring, abetting, aiding, or inducing the sale of counterfeit or infringing goods. However, the same would have to be determined on a case to case basis. Further, the provisions of the IT Act do not override the provisions of TM Act, unless there is a derogation between the said provisions. Accordingly, it has been held that the obligations under the TM Act would be independent and not get affected by the immunity claimed under the IT Act. Thus, it is settled law that safe harbour cannot be stretched to protect platforms that are active participants in infringement, as this would leave trademark owners without any remedy.

246. Further, in ***Neetu Singh (supra)*** the Court had considered the Rule 3 and 4 of the Intermediary Rules, 2021 *qua* obligations of intermediaries to protect IP rights. The Court had observed as under:

> *"45. This brings the Court to the defences taken by Telegram in its response to the prayer for disclosure. In this regard, this Court finds as under: […]*
>
> *(v) Telegram has also relied upon Rules 3 and 4 of the IT Guidelines. The said Rules read as under: […]*
>
> ***The above IT Guidelines are specific guidelines, which are provided in respect of "significant social media intermediaries" and the due diligence to be adhered to by them. These guidelines do not in any manner obviate the***

duty of Telegram as a platform to take all effective steps required to protect IP rights, including rights of copyright owners. This was also noted by the ld. Division Bench of this court in My Space Inc. v. Super Cassettes Industries Ltd., (2017) 236 DLT 478 (DB). The Court therein held as under:

> *"47. In this Court's opinion, Section 79 grants a measured privilege to an intermediary. However, that would not mean that the rights guaranteed under the Copyright Act are in any manner curtailed. All Section 79 does is regulates the liability in respect of intermediaries while the Copyright Act grants and controls rights of a copyright owner. Under the circumstances, it is difficult to conceive how one would pose a barrier in the applicability of the other.* ***The true intent of Section 79 is to ensure that in terms of globally accepted standards of intermediary liabilities and to further digital trade and economy, an intermediary is granted certain protections. Section 79 is neither an enforcement provision nor does it list out any penal consequences for non-compliance. It sets up a scheme where intermediaries have to follow certain minimum standards to avoid liability; it provides for an affirmative defence and not a blanket immunity from liability****."*

(vi) As held in Myspace (supra), the intermediary is to be granted safe harbour, so long as it complies with the requirements of law. ***In the present case, the infringement has to be nipped in the bud, without which Courts would have to continue to repeatedly pass injunction orders against mushrooming channels containing infringing content. The Court cannot perpetually supervise such***

> ***infringements and, thus, the origin and source of the infringing material has to be traced and such devices or persons involved in the infringement ought to face consequences in accordance with law, including being held liable for damages. That would not be possible if the source of such infringing copies, i.e., the details of the infringing channels are not disclosed.*** *Pertinently,* ***such production of details of infringing devices or persons or other sources, is not a comment on Telegram's liability and does not derogate from safe harbour provisions. In fact, it is aligned with the view of Telegram's claimed role as an intermediary, which claims to act as a conduit of information****."*

247. Thereafter, in ***Snapdeal (supra)***, a ld. Single Judge of this Court has considered the issue as to whether DNRs are intermediaries and what is the consequence of the paid services provided to the Registrants. The ld. Judge has categorically come to the conclusion that DNRs are intermediaries. However, providing of paid services, in the opinion of the ld. Single Judge, would render DNRs ineligible to claim the safe harbour protection, since the DNRs act commercially for a profit. The observations of the Court are set out below:

> *"68.* ***There is no dispute about the fact that the DNRs provide alternative domain names, in the event of the domain name that the aspiring registrant seeks being already taken, for a price and, in fact, charge higher prices for domain names which are more "in demand". Clearly, therefore, the DNRs act commercially for a profit****. In doing so, they use the allegedly infringing marks in the course of trade, by offering the domain names which constitutes the marks, for sale to aspiring registrants for a price. There is, therefore, clear user "in the course of trade", by the DNRs of the allegedly infringing domain*

names. More specifically, in the case of the plaintiff, the DNRs use the plaintiff's registered "SNAPDEAL" mark by offering the infringing domain names up to any aspiring registrant for a price. ***By doing so, the DNRs are clearly using, in the course of trade, the allegedly infringing marks. The contention, of learned Counsel for the DNRs, that any allegation of infringement by use in the course of trade of the allegedly infringing domain names, would only lie at the door of the registrants is, therefore, prima facie, misconceived and has to be rejected****."*

248. Insofar as the alternate domain names consisting of some trademarks are concerned, in ***Snapdeal*** the ld. Single Judge has held as under:

"87. I entirely agree. ***Infringement of intellectual property rights is not condonable in law. A registered trademark cannot be infringed, in view of the clear proscriptions contained in Sections 28 and 29 of the Trade Marks Act. There can be no argument against this. It is not open to anyone to contend that its activities are so carried out that it cannot guarantee against infringement. Nor can it lie in the mouth of anyone that it is practically not possible for it to carry out its activities in a manner which would not infringe others' intellectual property rights****. The contention of DNRs that the manner in which alternative domain names are provided, on their websites to prospective registrants, in the event of the domain names sought by the registrants being not available, is automated and that, therefore, they cannot ensure that such alternative domain names would not be infringing, is simply not acceptable.* ***Admittedly, the algorithm, on the basis of which the alternative domain names are made available, is devised by each individual DNR itself. It is the DNRs' responsibility to ensure that the alternative domain names do not infringe any registered trademark.***

The mere fact that a declaration to the said effect is also extracted from the prospective registrant is no insurance against the liability which would fall on the DNR, were it to be providing infringing alternative domain names. If the algorithm works in such a manner that there is a possibility of infringing alternative domain names being made available to an aspiring registrant, the DNR has to discontinue the use of such algorithm. If the consequence is that the DNR would not be able to provide alternatives, so be it. The law does not permit, or condone, its infraction.

88. There is no substance, therefore, in the contention of learned Counsel for the DNRs that, as the process by which alternative domain names are sourced from the Domain Name Registry is automated, they cannot vouchsafe to the alternative domain names not being infringing in nature. If that is the position, the DNRs have to discontinue providing alternative domain names or find some way or the other to ensure that infringing domain names are not provided. That the website of Defendant 1 does not provide any domain name containing the thread "GoDaddy" indicates that, in fact, this is possible.

[...]

91. ***Neither do the DNRs have any right to make available for registration, to aspiring registrants, domain names which infringe existing registered trademarks, nor does any registrant have a right to registration of such an infringing domain name****. If the Court were to grant the prayer, of the plaintiff, for an anticipatory injunction, restraining the DNRs from making available, to any aspiring registrant, any domain name containing the 'SNAPDEAL' string/thread, it would be on the premise that*

any such spring/thread would, prima facie, be infringing in nature. That being so, any such injunction would not affect, judicially, any right of the DNRs either, as no DNR can claim, as of right, an entitlement to provide, to aspiring registrants, a domain name which infringes an existing trademark, especially for profit.

[...]

98. ***In all such cases, however, the DNRs, by the application of the algorithm derived by whom the infringing domain names are becoming available to prospective registrants, would themselves be "infringers", within the meaning of Section 29 of the Trade Marks Act, and liable in that regard****. In order to avoid such liability, in my opinion, the DNRs would either have to modulate their algorithms in such a way as not to make available, to prospective registrants, potentially infringing alternatives – as Defendant 1 has apparently done in respect of its own domain name – or avoid providing alternative domain names altogether.* ***A situation in which the algorithms of the DNRs make available, to prospective registrants, infringing domain names, leaving the proprietors of the infringed trade marks to repeatedly knock at the doors of the Court cannot be allowed to continue in perpetuo."***

249. Thus, it is settled that the non-implementation of steps to prevent trademark infringement coupled with various means and methods adopted by the DNRs to maximize their revenues would actually lead to non-grant of safe harbour protection in respect of the said DNRs. Further, as is clear from the screenshots extracted hereinabove, the DNRs continue to promote alternative infringing domain names, several of which are clearly *prima facie* infringing the

trademarks of the Plaintiffs. In such a situation, not only shall the concerned DNRs lose the safe harbour protection, the said DNRs would be liable to be treated as infringers against whom reliefs would be liable to be claimed. Accordingly, such DNRs in an appropriate case could be held to be liable to pay monetary damages as well.

250. Having considered the issue of safe harbour protection to DNRs and Registry Operators, it would also be necessary to consider whether a non-compliant entity can itself be blocked from providing services in India. The submission on behalf of DNRs is that non-compliance of orders of the Court would not satisfy the high threshold of 'public order' which is one of the grounds upon which the blocking order can be issued. The DNRs and Registry Operators have relied in support of broader protections as Intermediary on the decisions of the Supreme Court in ***Shreya Singhal (supra)*** and in ***Visaka Industries (supra).***

251. The Court has considered the said decisions. In ***Shreya Singhal (supra)*** the Supreme Court was considering a challenge to Section 66A and Section 69A of the IT Act. The Supreme Court has analysed the validity of the said sections in light of the freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India. In the course of the said analysis the Supreme Court has considered the scope of the term 'public order' which is one of the reasonable restrictions on the freedom of speech and expression mentioned in Article 19(2) of the Constitution of India. The relevant portion of the said decision is extracted hereunder:

> "***36.*** *In Supt., Central Prison v. Ram Manohar Lohia this Court held that public order is synonymous with public*

safety and tranquility; it is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State. This definition was further refined in Ram Manohar Lohia v. State of Bihar, where this Court held:

> *"It will thus appear that just as 'public order' in the rulings of this Court (earlier cited) was said to comprehend disorders of less gravity than those affecting 'security of State', 'law and order' also comprehends disorders of less gravity than those affecting 'public order'. One has to imagine three concentric circles. Law and order represents the largest circle within which is the next circle representing public order and the smallest circle represents security of State. It is then easy to see that an act may affect law and order but not public order just as an act may affect public order but not security of the State."*

37. *In Arun Ghosh v. State of W.B., Ram Manohar Lohia case was referred to with approval in the following terms:*

"... In Ram Manohar Lohia case this Court pointed out the difference between maintenance of law and order and its disturbance and the maintenance of public order and its disturbance. ***Public order was said to embrace more of the community than law and order. Public order is the even tempo of the life of the community taking the country as a whole or even a specified locality. Disturbance of public order is to be distinguished from acts directed against individuals which do not disturb the society to the extent of causing a general disturbance of public tranquillity. It is the degree of disturbance and its effect upon the life of the community in a locality which determines whether the***

disturbance amounts only to a breach of law and order. *Take for instance, a man stabs another. People may be shocked and even disturbed, but the life of the community keeps moving at an even tempo, however much one may dislike the act. Take another case of a town where there is communal tension. A man stabs a member of the other community. This is an act of a very different sort. Its implications are deeper and it affects the even tempo of life and public order is jeopardised because the repercussions of the act embrace large sections of the community and incite them to make further breaches of the law and order and to subvert the public order.* ***An act by itself is not determinant of its own gravity. In its quality it may not differ from another but in its potentiality it may be very different.*** *Take the case of assault on girls. A guest at a hotel may kiss or make advances to half a dozen chamber maids. He may annoy them and also the management but he does not cause disturbance of public order. He may even have a fracas with the friends of one of the girls but even then it would be a case of breach of law and order only. Take another case of a man who molests women in lonely places. As a result of his activities girls going to colleges and schools are in constant danger and fear. Women going for their ordinary business are afraid of being waylaid and assaulted. The activity of this man in its essential quality is not different from the act of the other man but in its potentiality and in its effect upon the public tranquillity there is a vast difference. The act of the man who molests the girls in lonely places causes a disturbance in the even tempo of living which is the first requirement of public order. He disturbs the society and the community. His act makes all the women apprehensive of their honour and he can be said to be causing disturbance of public order and not merely committing individual actions which may be taken note of by the criminal prosecution agencies.* ***It***

means therefore that the question whether a man has only committed a breach of law and order or has acted in a manner likely to cause a disturbance of the public order is a question of degree and the extent of the reach of the act upon the society*. The French distinguish law and order and public order by designating the latter as order publique. The latter expression has been recognised as meaning something more than ordinary maintenance of law and order. Justice Ramaswami in Pushkar Mukherjee v. State of W.B. [(1969) 1 SCC 10]* ***drew a line of demarcation between the serious and aggravated forms of breaches of public order which affect the community or endanger the public interest at large from minor breaches of peace which do not affect the public at large****. He drew an analogy between public and private crimes. The analogy is useful but not to be pushed too far. A large number of acts directed against persons or individuals may total up into a breach of public order. In Ram Manohar Lohia case [Ram Manohar Lohia v. State of Bihar, (1966) 1 SCR 709 : AIR 1966 SC 740 : 1966 Cri LJ 608] examples were given by Sarkar, and Hidayatullah, JJ. They show how similar acts in different contexts affect differently law and order on the one hand and public order on the other.* ***It is always a question of degree of the harm and its effect upon the community. The question to ask is : Does it lead to disturbance of the current of life of the community so as to amount to a disturbance of the public order or does it affect merely an individual leaving the tranquillity of the society undisturbed? This question has to be faced in every case on facts. There is no formula by which one case can be distinguished from another****."*

[...]

38. *This decision lays down the test that has to be*

formulated in all these cases. ***We have to ask ourselves the question: does a particular act lead to disturbance of the current life of the community or does it merely affect an individual leaving the tranquility of society undisturbed****? […]"*

252. Accordingly, the test for whether 'public order' has been affected by an act would be to consider the gravity and effect of the said act on the society at large and whether the same would disturb the tranquillity of the society. Applying this test to individual cases of mere IP infringement may not satisfy the high threshold of public order and instead would be an issue of law and order, since, the same may not have disturb the society at large. However, where there is consistent violation of IP rights along with attempts to defraud innocent public of their hard earned monies and also assist in commission of offences, the same would have a significant impact upon the society at large. In today's age of rapid evolution of technology it is not uncommon for new methods of frauds to be reported. It is also often seen that by the time the LEAs catch up with the fraudsters and are able to comprehend the methods used, the fraudsters move on and start defrauding the public through some newer method. Given that such frauds are increasing in number day by day, it is now more than ever necessary to build and maintain trust in the manner in which consumers interact and connect with brands and companies. If the consumer cannot trust the authenticity of the website or domain name she/he has accessed, which would be a logical consequence of the large scale frauds brought to the attention of the Court in the present batch of suits, then it would definitely disturb the economic interests of the businesses and also create disturbance to members of the general public and

society. Therefore, in the opinion of the Court, in light of the large scale frauds which are being committed, directions of the Court cannot be rendered ineffective by non-compliant DNRs and Registry Operators, for which the Court may direct the competent authorities to block the services of the non-compliant DNRs itself in order to ensure compliance.

253. Insofar as those entities who are operating from foreign jurisdictions and have refused to comply with the orders of Indian Courts are concerned, this Court in ***Neetu Singh (supra),*** the Court has already considered a similar situation. In the said case, Telegram - a social media intermediary having its servers in Singapore and operating from foreign shores had refused to comply with the order of this Court directing it to provide information of concerned infringers. The Court considered the following factors before holding it to be a competent Court to direct Telegram to disclose information:

(i) Telegram is one of the most popular messaging applications in India with subscriber base running into millions of users;

(ii) Infringement of copyright was unabashedly continued within India;

(iii) Accounts sharing the infringing material were created in India;

(iv) High possibility of the persons controlling the infringing accounts would be in India along with the devices involved in the dissemination of the material;

(v) Cloud computing permits access to information beyond jurisdictions, including in India, irrespective of where the data centres are located. Thus, conventional concepts of territoriality no longer exist.

(vi) Telegram is actively making its services accessible in India along with

offering paid services to earn revenue.

(vii) Reliance on the decisions of the Supreme Court in ***Indian Bank v. Satyam Fibres (India) (P) Ltd., (1996) 5 SCC 550*** and ***Krishan Yadav v. State of Bihar, AIR 1994 SC 2166,*** which held that High Courts are vested with inherent powers to enable themselves to maintain their dignity, and secure obedience to their process and rules and give effective reliefs.

In the opinion of the Court, each of the above factors would squarely apply in respect of DNRs and Registry Operators, who not only provide services in India but are involved in generating significant revenues from numerous customers in India. Thus, applying the same factors, it is clear that even in respect of the ICANN Agreements, Indian Courts would be courts of competent jurisdiction to issue directions to DNRs and Registry Operators for grant of appropriate relief.

Dynamic and Dynamic + Injunctions

254. In ***UTV Software Communication (supra)*** this Court has already recognized the grant of dynamic injunctions as being necessary in such cases. The observations read as under:

> *"93. Undoubtedly, website blocking is 'no silver bullet' in the fight against digital piracy, but it should at least be one of the lead bullets, alongside other measures such as partnering with Internet ad companies, domain seizures, and other efforts to prosecute owners of pirate sites. HOW SHOULD THE COURT DEAL WITH THE 'HYDRA HEADED' 'ROGUE WEBSITES WHO ON BEING BLOCKED, ACTUALLY MULTIPLY AND RESURFACE AS REDIRECT OR MIRROR OR ALPHANUMERIC WEBSITES?*

94. Now, the question that arises for consideration is how should courts deal with 'hydra headed' websites who on being blocked, actually multiply and resurface as alphanumeric or mirror websites. In the present batch of matters though this Court had injuncted the main website by way of the initial injunction order, yet the mirror/alphanumeric/redirect websites had been created subsequently to circumvent the injunction orders.

95. It is pertinent to mention that in Greek mythology the Hydra also called Lernaean Hydra is a serpent-like monster. The Hydra is a nine-headed serpent like snake. It was said that if you cut off one hydra head, two more would grow back.

96. Critics claim that website blocking is an exercise in futility as website operators shift sites-the so-called "whack-a-mole" effect.

97. Internationally, there has been some recent development to deal with the aforesaid menace in the form of a "Dynamic Injunction" though limited to mirror websites.

98. The High Court of Singapore in the case of Disney Enterprise v. Ml Ltd., (2018) SGHC 206 has after discussing the cases of 20th Century Fox v. British Telecommunications PLC, (2012) 1 All ER 869 and Cartier International AG v. British Sky Broadcasting (supra), held that the applicant was not obligated to return to court for an order with respect to every single IP address of the infringing URLs already determined by the Court. The Court held as under:—

"38 I found that the court has the jurisdiction to issue

a dynamic injunction given that such an injunction constitutes "reasonable steps to disable access to the flagrantly infringing online location". This is because the dynamic injunction does not require the defendants to block additional FIOLs which have not been included in the main injunction. It only requires the defendants to block additional domain names, URLs and/or IP addresses that provide access to the same websites which are the subject of the main injunction and which I have found constitute FIOLs (see [19] - [29] above). Therefore, the dynamic injunction merely blocks new means of accessing the same infringing websites, rather than blocking new infringing websites that have not been included in the main injunction.

39 In fact, under the dynamic injunction applied for in the present case, the plaintiffs would be required to show in its affidavit that the new FQDNs provide access to the same FIOLs which are the subject of the main injunction before the defendants would be required to block the new FQDNs (see [6] above) ... xxx xxx xxx

42. In relation to S 193DB(3)(d) of the Copyright Act, ie, the effectiveness of the proposed order, the dynamic injunction was necessary to ensure that the main injunction operated effectively to reduce further harm to the plaintiffs. This is due to the ease and speed at which circumventive measures may be taken by owners and operators of FIOLs to evade the main injunction, through for instance changing the primary domain name of the FIOL. Without a continuing obligation to block additional domain names, URLs and/or IP addresses upon being informed of such

sites, it is unlikely that there would be effective disabling of access to the 53 FIOLs."
(emphasis supplied)

99. Though the dynamic injunction was issued by the Singapore High Court under the provisions of Section 193 DDA of the Singapore Copyright Act, and no similar procedure exists in India, yet in order to meet the ends of justice and to address the menace of piracy, this Court in exercise of its inherent power under Section 151 CPC permits the plaintiffs to implead the mirror/redirect/alphanumeric websites under Order I Rule 10 CPC as these websites merely provide access to the same websites which are the subject of the main injunction.

*100. **It is desirable that the Court is freed from constantly monitoring and adjudicating the issue of mirror/redirect/alphanumeric websites and also that the plaintiffs are not burdened with filing fresh suits. However, it is not disputed that given the wide ramifications of site-wide blocking orders, there has to be judicial scrutiny of such directions and that ISPs ought not to be tasked with the role of arbiters, contrary to their strictly passive and neutral role as intermediaries.***

101. Consequently, along with the Order I Rule 10 application for impleadment, the plaintiffs shall file an affidavit confirming that the newly impleaded website is a mirror/redirect/alphanumeric website with sufficient supporting evidence. On being satisfied that the impugned website is indeed a mirror/redirect/alphanumeric website of injuncted Rogue Website(s) and merely provides new means of accessing the same primary infringing website, the Joint Registrar shall issue directions to ISPs to disable access in India to such mirror/redirect/alphanumeric websites in terms of

the orders passed.

102. It is pertinent to mention that this Court has delegated its power to the learned Joint Registrar for passing such orders under Section 7 of the Delhi High Court Act, 1966 read with Chapter II, Rule 3(61) read with Rule 6 of the Delhi High Court (Original Side) Rules 2018. The said provisions are reproduced hereinbelow:—

> *"3. Powers of the Registrar- The powers of the Court, including the power to impose costs in relation to the following matters, may be exercised by the registrar: (61) Such other application, as by these Rules are directed to be so disposed of by the Registrar, but not included in this Rule and any other matter, which in accordance with orders or directions issued by Court, is required to be dealt with by the Registrar.*
>
> *6. Delegation of the Registrar's Power - The Chief Justice and his companion Judges may assign or delegate to a Joint Registrar, Deputy Registrar or to any officer, any functions required by these Rules to be exercised by the Registrar.*

103. In the event, any person is aggrieved by any order passed by the Registrar, the remedy for appeal is provided and may be availed of under Rule 5 of Chapter II of the Delhi High Court (Original Side) Rules, 2018 reproduced hereinbelow:—

> *"5. Appeal against the Registrar's orders.- Any persons aggrieved by any order made by the Registrar, under Rule 3 of this Chapter, may, within fifteen days of such order, appeal against the same to the Judge in Chambers. The appeal shall be in the form of a petition bearing court fees of Rs. 2.65."*

255. This has also been extended to works, which are yet to come into existence in ***Universal City Studios LLC. v. Dotmovies.baby., CS(COMM) 514/2023*** *(order dated 9th August, 2023)* by grant of a **Dynamic +** injunction. The relevant portion of the said order reads as under:

> *"16. The dynamism of the injunction, by itself, in one country or another may not, however be sufficient to protect copyright owners.* ***There is an imminent need to evolve a global consensus in this regard inasmuch as despite ISPs blocking these websites, the said websites can be accessed through VPN servers, and other methods to which the long arm of the law cannot extend etc.***
>
> *17.* ***Any injunction granted by a Court of law ought to be effective in nature. The injunction ought to also not merely extend to content which is past content created prior to the filing of the suit but also to content which may be generated on a day-to-day basis by the Plaintiffs.*** *Thus, though, in a usual case for copyright infringement, the Court firstly identifies the work, determines the Copyright of the Plaintiff in the said work, and thereafter grants an injunction, owing to the nature of the malafide, there is a need to pass injunctions which are also dynamic qua the Plaintiff as well, as it is seen that upon any film or series being released, they may be immediately uploaded on the rogue websites, causing immediate monetary loss. Copyright in future works comes into existence immediately upon the work being created, and Plaintiffs cannot be forced to approach the Court for each and every film or series that is produced in the future, to secure an injunction against piracy.*
>
> *[...]*

19. ***As innovation in technology continues, remedies to be granted also ought to be calibrated by Courts. This is not to say that in every case, an injunction qua future works can be granted. Such grant of an injunction would depend on the fact situation that arises and is placed before the Court****.*

20. In the facts and circumstances as set out above, an ex parte ad interim injunction is granted restraining the Defendants, who are all rogue websites, from in any manner streaming, reproducing, distributing, making available to the public and/or communicating to the public any copyrighted content of the Plaintiffs including future works of the Plaintiffs, in which ownership of copyright is undisputed, through their websites identified in the suit or any mirror/redirect websites or alphanumeric variations thereof including those websites which are associated with the Defendants' websites either based on the name, branding, identity or even source of content. ***To keep pace with the dynamic nature of the infringement that is undertaken by hydra-headed websites, this Court has deemed it appropriate to issue this 'Dynamic+ injunction' to protect copyrighted works as soon as they are created, to ensure that no irreparable loss is caused to the authors and owners of copyrighted works, as there is an imminent possibility of works being uploaded on rogue websites or their newer versions immediately upon the films/shows/series etc. The Plaintiffs are permitted to implead any mirror/redirect/alphanumberic variations of the websites identified in the suit as Defendants Nos. 1 to 16 including those websites which are associated with the Defendants Nos. 1 to 16, either based on the name, branding, identity or even source of content, by filing an application for impleadment under Order I Rule 10 CPC in the event such websites merely provide new means of***

> ***accessing the same primary infringing websites that have been injuncted. The Plaintiffs are at liberty to file such an impleadment application based on their copyrighted works, including future works, when the need so arises. Upon filing such application before the Registrar along with an affidavit with sufficient supporting evidence seeking extension of the injunction to such websites, to protect the content of the Plaintiffs, including future works, the injunction shall become operational against the said websites and qua such works. If there is any work in respect of which there is any dispute as to ownership of copyright, an application may be moved by the affected party before the Court, to seek clarification.****"*

256. It would also be relevant to note that based on the above decisions, this Court in ***Burger King Corpn. (supra)***[17]***,*** one of the suits in the batch, has relied on the above orders to grant reliefs to the Plaintiff. The said order has also been relied by the DNRs in respect of the directions for blocking that were passed to NIXI. The relevant portion of the said order reads as under:

> *"13. Keeping in mind the above legal position as also considering the nature of this mater, the Court has perused the screen shots of the websites i.e. Documents 3 and 4 with this Application. The use of the 'BURGER KING' in this manner and calling for franchises could result in large scale fraudulent payments of money to the operators of these websites. Such websites are noted to surface frequently and periodically. Additionally, the deceptive nature of their operations extends beyond mere trade mark infringement, raising concerns about consumer safety and ethical business practices.*
>
> *14. In light of these circumstances, considering the broader*

[17] **Burger King Corpn. v. Swapnil Patil, CS(Comm)303/2022** (decided on 4th December, 2023)

implications of such Defendants' actions, in order to safeguard both the integrity of the market and the welfare of consumers, the said websites and their operators are restrained from using the said domain names or any other domain names which bear the mark 'BURGER KING' as also the words 'BURGER' and 'KING' together.

15. In addition, if any other domain names/websites offering fake franchises are noticed/ discovered by the Plaintiff bearing the mark 'BURGER KING', the Plaintiff is free to file an affidavit along with the application for impleadment under Order I Rule 10 CPC. The Plaintiff is permitted to implead any mirror/redirect/alphanumeric variations of the websites identified in the suit as Defendant websites which are associated with the Defendants either based on the name, branding, identity etc., by filing the application. The Joint Registrar may examine the documents filed with the same and direct extension of the injunction orders to the said domain names as well. MEITY/DoT shall, upon receiving of any information in respect of fake franchises/websites shall immediately issue blocking orders in respect of the said websites.

16. The above-mentioned two domain name websites shall also be blocked by MEITY and the Internet Service Providers (hereinafter, ISPs) shall give effect to these orders. National Internet Exchange of India (hereinafter, NIXI) shall give effect to this order immediately and block/suspend the said domain names.

17. Further, GoDaddy.com LLC shall lock/suspend the domain name www.burgerkingfoodindia.com and www.burgerkingfranchiseindia.co.in. They shall also provide the details of the registrants within one week, including the payment details, if any, which are available with them to ld. Counsel for the Plaintiff."

257. In the above background, the nature of the relief that is to be granted, deserves to be considered. Insofar as the Plaintiffs are concerned, they have prayed for relief, in effect, seeking injunction against existing infringing domain names as also blocking of registration of future domain names consisting of the Plaintiff's well known mark and registered trademarks. In addition, reliefs are sought against the Registry Operators from allowing the infringing domain names to resolve into websites. The prayer is also made for transfer of the domain names and for implementation of locking and blocking of the domain names. It is argued that trademarks, which are protected by the Court, ought to be also given the services of being included into the trademark clearing house so that notice of any new infringing registration, can be received.

258. In these very suits, it is seen that there are multiple domain names being added during the pendency of these suits. For example, in the case of ***CS(Comm) 373/2020*** titled ***ITC vs. Ashok Kumar & Anr.***, 286 domain names have been added. The numbers of domain names added in some of the matters during the pendency of the suit are set out below:

Sr. No	**Details of the Suit**	**Number of Infringing Domain Names**
1.	Gujarat Cooperative Milk Marketing Federation Ltd and Anr. vs Amul-Franchise.in & Ors, CS (COMM) NO. 350/2020	79
2.	*Bajaj Finance Limited vs. Registrant Of www.bajaj-finserve.org & Ors.* *CS (COMM) NO. 228/2021*	222

3.	*Fashnear Technologies Pvt Ltd vs. Meesho Online Shopping Pvt Ltd & Anr* *CS (COMM) 475 OF 2022*	27
4.	Ultratech Cement Limited & Anr. vs. ww.ultratechcements.com & Ors. *C.S. (COMM) NO. 298 OF 2019*	62
5.	*Godrej Properties Ltd. vs. Ashok Kumar & Anr.,* *CS (COMM) NO. 154 OF 2021*	91
6.	*McDonald's Corporation & Anr. v. National Internet Exchange of India & Ors.* *C.S. COMM NO. 324 OF 2020*	110
7.	*PB Fintech Pvt. Ltd. V Policy Bazar Finance & Ors.* *CS(COMM) 471/2020*	47

259. A perusal of the infringing domain names would show that the DNRs are permitting registration of well-known marks, famous marks, global brands, names of corporate house names to be registered, thereby, resulting in misuse. It is a matter of fact that the same rule cannot be applied for all categories of marks. The relief, therefore, would have to be moulded depending upon the nature and character of the mark.

260. There are various categories of trademarks that are being sought to be protected in these commercial suits including invented and fanciful marks, descriptive marks which have acquired a secondary meaning, as also dictionary words which have been arbitrarily adopted and have become well known trade marks. The nature of protection to be awarded to the different categories of marks is not the same. At the highest end of the spectrum are invented fanciful and arbitrary marks which deserves a high level of protection. The other kinds of

marks may require greater scrutiny before injunctions are granted. Accordingly, depending upon the nature of the marks, the relief would have to be moulded.

261. However, insofar as the disclosure of registrant details and related data is concerned, there can be no doubt that the process requires to be streamlined and immediate access to the said details is made available. In the opinion of this Court, the broader enforcement of law needs to be given primacy in these cases where there is apparent illegality in registration of the domain names which consists of well-known trademarks or brand names. Infringing domain names deserve to be restrained. Insofar as future registrations are concerned, well-known trademarks deserve to be protected. For the said purpose, DNRs can be directed to access the list of well-known trademarks from Controller General of Patents, Designs and Trade Marks (hereinafter "*CGPDTM*") office and add the said marks into a blocking/Reserved list. Technological solutions would have to be given effect to by DNRs to ensure that the relief is effective. If, however, any genuine Registrant, who wishes to criticize the Plaintiff or its business, seeks a claim for a specific domain name, such a dispute would have to be resolved in a Court of Law.

262. Further, insofar as privacy aspects and disclosure of personal details of Registrants is concerned, the relevant agreement between ICANN and DNRs as also the Registry and the DNRs recognizes that if a person with legitimate interest approaches the DNR, the said data can be disclosed. The same would now be governed by the applicable laws, which in terms of domain names registered in India would be the DPDP Act. It is, thus, held that whenever details are sought by any IP owner or by any LEA on behalf of the IP owners or upon

occurrence of cyber fraud, the same constitutes legitimate interest and the Registry Operators and the DNRs, which may be having the data, ought to mandatorily disclose the same.

VII. SUMMARY AND CONCLUSIONS

263. In the age of technology and internet, domain names/websites form the ***online soul*** of a business, and their distinctive character has to be protected. Repeated cases of cyber fraud, cyber terrorism, and other forms of online fraudulent activity traces back to registration of infringing domain names. Misuse of domain names and website content deserves to be dealt with stringent action as, in addition to infringing the interest of the owner of the mark/brand, it also endangers the larger public interest. Such stringent action would be required to be taken by or against various parties to maintain the integrity of the domain name system. Such parties include:

a. **Domain Name Registrants** – Person registering the domain name;

b. **Domain Name Registrars (DNRs)** – Entity enabling the registration of the domain name;

c. **Domain Name Registry Operator** – The Registry under which the DNR operates;

d. **ICANN** – Internet Corporation on Assigned Names and Numbers – the overall regulator of the domain name system;

e. **Banks** – where the bank accounts are opened by infringers;

f. **Reserve Bank of India** – Banking regulator which had to take steps to curb fraudulent activities through banking channels;

g. **Telecom Service Providers** – Companies which provide SIM cards and associated telecom services;

h. **MeitY and DoT** – Ministries which oversee the access to the internet in India and also regulate the internet/telecom service providers;

i. **Law Enforcement Agencies** – Police and other investigating agencies.

264. One of the major issues that was common in these matters was the lack of safeguards at certain key junctures in the financial transaction system which enabled unscrupulous entities to defraud innocent persons by opening fake bank accounts, passing off as the actual brands/companies. The act of fraudulently collecting money by setting up infringing websites and fake bank accounts has become prolific. One of the root causes for the same was lack of customer knowledge as to who is the recipient of the payment being made. The bank account is usually in the name of an individual who is collecting money by posing as a well-known corporate house/business. This is now sought to be cured by the RBI during the course of these litigations, under directions from this Court, by mandating the ***'Beneficiary Bank Account Name Lookup'***. It is imperative for all banks, including both private and public sector banks, to implement this facility especially in the case of online payments using the UPI system through payment apps such as Google Pay, Paytm, etc. In the case of RTGS and NEFT the said facility of knowing the recipients' name is stated to have already been implemented. If the name of the beneficiary becomes visible, the customers could exercise caution and the same may also act as a warning if there is a mismatch in the name of the account holder from the business they seek

to impersonate.

265. In addition to the above, another difficulty faced by the Law Enforcement Agencies ('***LEA***') in investigating financial frauds was the lack of co-operation from the banks. This issue has also been resolved pursuant to the directions of this Court, whereby the Central Intelligence and Economic Bureau issued the Standard Operating Procedure dated 31st May, 2024 for processing of requests from LEAs by the banks. The same has also been communicated to all the banks by the Indian Banks' Association on 3rd June, 2025. Thus, it is now mandatory for all banks to cooperate with LEAs in terms of the SOP dated 31st May, 2024 as issued by Central Intelligence and Economic Bureau.

266. The financial frauds by passing off as reputed brands and corporate houses is a direct consequence of the availability and use of fraudulent and fake domain names. The domain name system operates in a pyramidical structure of hierarchy with the inclusion of ICANN at the top, followed by the Registry Operators, the DNRs and the Registrants. Each of the said entities have a specific role in the domain name system which is governed by the set of agreements drafted by ICANN, such as the Registrar Accreditation Agreements, the Registry-Registrar Agreements, etc.

267. Several significant obligations have been imposed upon the Registry Operators and DNRs under the ICANN Agreements to ensure that registration of a domain name does not violate the rights of a third party. The Registry Operators must comply with ICANN's policies, bye-laws, and the codes of conduct. They are required to operate the WHOIS services in the format prescribed in Specification 4, along with observing reserved names listed in

Specification 5. They are obligated to take reasonable steps to investigate and respond to requests from law-enforcement or governmental bodies regarding illegal conduct involving their TLDs. They must additionally implement **Rights Protection Mechanisms** under Specification 7, including use of the **Trademark Clearinghouse database**, which alerts both registrants and trademark owners when a domain identical to a recorded trademark is sought to be registered, enabling early detection of potential trademark conflicts.

268. The DNRs ought to submit registered-name data to the Registry Operator, provide public query-based access to essential WHOIS/RDDS information, make registrant data available for ICANN's inspection, comply with applicable laws and governmental regulations, avoid registering reserved names, verify and periodically re-verify Registrant contact information, investigate inaccuracies, and act promptly against DNS abuse or illegal activity. They ought to face termination of the accreditation agreement if a Court finds they permitted illegal activity or failed to comply with Court's orders, or if ICANN determines that the DNRs engaged in bad-faith trademark-conflicting registrations. Additionally, they are obliged to follow ICANN's WHOIS Accuracy Specification, validating address, email, and phone formats, and verifying email or telephone numbers through tool-based authentication, and must suspend or terminate domain names where registrants wilfully provide inaccurate information and fail to correct it within 15 days.

269. The DNRs play a critical role in maintaining the integrity of the domain names/website system and in preventing misuse of the same. However, the privacy protect feature extended by DNRs to registrants is acting as a cloak to

hide the identity of those perpetrating illegal and unlawful acts on the internet. This is further exacerbated by the failure of the DNRs to collect proper information of the Registrants, since, even where the privacy protection has not been provided/availed, the information with the DNRs is entirely insufficient to identify the Registrants.

270. Most DNRs in the present batch of matters do not have any proper contact details of the concerned Registrants including name, address, mobile number, etc. Even the email addresses which are used sometimes could be through unauthorized and banned email service providers. Although, the ICANN agreements, as also the NIXI Agreements, mandate collection of several contact details of the Registrant and verification of the same, as on date, the only requirement sought by DNRs for registering a domain name is an email address, which is grossly insufficient to prevent cyber fraud, cybercrime and misuse of domain names. Thus, it is necessary to mandate that all DNRs offering their services in India shall collect the details of the Registrants and perform a e-KYC verification in the manner in which NIXI already mandates in India. It is noted that the Registrar Accreditation Agreements with ICANN also mandate collection of email address and mobile number, and verification of the same by means of OTP under Clause 1(f) of the RDDS Accuracy Program Specification. The MHA also supports the reflection of administrative contact details, payment information, IP addresses, SSL certificate provider details and KYC details in the WHOIS database.

271. It is also clear from the changes in the privacy policy of ICANN that DNRs and Registry Operators cannot deny disclosure of Registrant's details by taking

blanket cover under the provisions of GDPR. The applicable privacy law would govern the relevant considerations in each case, and accordingly, the data collected from Registrants in India would be governed in terms of the DPDP Act and its allied Rules.

272. Further, implementation of orders passed by Courts by DNRs is crucial for preventing misuse as also for maintaining law and order. However, many DNRs do not have offices in India. Some of the servers could also be located abroad. Whenever an infringing domain name is found, one of the most challenging aspect is to serve the domain name registrar and enforcement of the order of the Court. Even IP owners find it challenging to obtain basic details of the Registrant. Moreover, the LEAs have a challenging responsibility in preventing cyber frauds on the internet and hence they require cooperation from banks, financial institutions, DNRs, domain name registries as also IP owners.

273. The Intermediary Rules, 2021 mandate appointment of Grievance Officers by all intermediaries. All DNRs who offer their domain names registration or ancillary services ought to appoint Grievance Officers who are located in India and publish their email addresses, mobile numbers and other contact details so that they can be contacted for the purpose of obtaining relevant information of the Registrant as also for implementing orders passed by Courts and to provide information to LEAs.

274. In these set of cases, all three stake holders/custodian of internet domain name system, namely, ICANN, Registry Operators and DNRs have been heard. It is clear that all DNRs have a mandate to implement orders passed by Courts and cannot insist upon orders from local Courts of countries where they are

located for disclosure of information or suspending a domain name etc.

275. Accordingly, service of DNRs, Registries Operators and other intermediaries, if done through email on the details of the relevant Grievance Officer ought to be sufficient service for compliance with the requirement under the law. Furthermore, service on Registrants through the email address provided to the DNRs would also be sufficient, as in most cases, correct postal addresses are not available.

276. Further, the agreements that are entered into between ICANN, Registry Operators and DNRs would show that DNRs and Registry Operators have the competence and technological wherewithal to prevent registration of domain names of well-known marks and reputed brands, if the competent Court directs. Some of the Registries such as Registry Services LLC offer services such as ***Global Block*** and ***Global Block*** +, in support with the Brand Safety Alliance LLC (a GoDaddy group company), which establish this position. The Registry Operators also have the capability of implementing the '*Extensible Provisioning Protocol'* Status Codes, which would result in similar effect as intended by the Court through its directions for blocking/suspending/locking the infringing website. Many DNRs and other intermediaries do not merely offer domain name registration services, but they also provide add-on services, auction services, alternative domain names, etc. The various services provided by the DNRs through which significant revenue is also generated are:

(i) Offering domain names with varying extensions/suffixes of well-known brands, marks on premium rates.

(ii) Offering certain domain names categorised as 'premium' which are

sold at exorbitant prices.

(iii) Some Registry Operators offer services of blocking of domain names as premium services for which payments would have to be made by the respective IP owners.

(iv) By offering marketing and Search Engine Optimization services to promote websites/domain names including even illegal and fraudulent websites/domain names consisting of third-party mark.

(v) By putting infringing domain names in the common pool so that revenues can be earned repeatedly, though said domain names have been declared to be infringing.

(vi) By adopting discriminatory practices in respect of entities and marks with whom they have special arrangements.

(vii) By offering after market services in domain name

(viii) By operating domain name auction services whereby, the DNRs promote buying and selling of domain names as a way of investment. In effect this promotes monetising of the domain names even where the same violates the rights of third parties.

(ix) By providing brokerage services for assisting a new Registrant wishing to obtain an already registered domain name, purchase the same and transfer it to the new Registrant.

(x) A number of the DNRs also provide webhosting, marketing, and other support services to infringing domain names, thereby garnering substantive revenues. However, these facts are not usually disclosed to the Court.

(xi) By not implementing technologies, which are available with them for ensuring that well known marks and registered trade marks are not misused to prevent cyber fraud, only with a view to maximise revenues.

The above services not only generate revenue of the DNRs and Registry Operators but also help persons with illegal and unlawful motives to register domain names which are similar to well-known marks, brands, house-marks, etc. Such DNRs may, therefore, not merely be considered as intermediaries but as complicit in actively enabling infringement.

277. It is a settled position in law in India that registration of an infringing domain name would not be permissible as there is every likelihood that the same could lead to diversion of users from the genuine website to the infringing one.

278. Thus, the non-implementation of steps to prevent trademark infringement coupled with various means and methods adopted by the DNRs to maximize their revenues would actually lead to non-grant of safe harbour protection in respect of the said DNRs. Further, as is clear from the screenshots extracted hereinabove, the DNRs continue to promote alternative infringing domain names, several of which are clearly *prima facie* infringing the trademarks of the Plaintiffs. In such a situation, not only shall the concerned DNRs lose the safe harbour protection, the said DNRs would be liable to be treated as infringers against whom reliefs would be liable to be claimed. Accordingly, such DNRs in an appropriate case could be held to be liable to pay monetary damages as well.

279. Moreover, the failure of DNRs to comply with Court orders would necessitate stringent measures to be taken, including blocking of their services

in India that may be ordered by Courts, as where there is consistent violation of IP rights along with attempts to defraud innocent public of their hard earned monies and also assist in commission of offences, the same would have a significant impact upon the society at large, leading to disrupting the public order.

280. Offering of privacy by default to registrants is one of the reasons for proliferation of illegal domain names. Thus, unless and until a registrant requests for privacy protect, the same should not be offered as a default mechanism.

281. The Government and various institutions including Central Government, State Governments, Autonomous Institutions, Judicial Bodies, Tribunals, Income Tax Department, GST Department and Critical Bodies such as Army, Navy, Airforce, ISRO, Atomic Research Bodies, etc. ought to create their own list of names that can be misused so that such domain names can be placed in the reserved list.

282. In all these suits where about 1132 infringing domain names have been impugned, barring one or two domain names, no *bonafide* registrant come forward claiming legitimate right to use the infringing domain names. This itself shows that the infringing domain names are being proliferated only for unlawful and illegal purposes. Thus, there is an urgent necessity for directions to passed to ensure the trust of the consumers as also the interest of businesses is protected, and no party is permitted to commit frauds due to failure of sufficient safeguards in the system.

VIII. DIRECTIONS

283. Under these circumstances, considering the above mentioned discussion

the following directions are issued:

(A) ***Directions to DNRs and Registry Operators***

(i) The DNRs and Registry Operators shall, henceforth, not resort to masking of details of the registrants, administrative contact and technical contact on a default basis as an 'opt-out' system. At the time of registration of the domain names, a specific option shall be provided for the Registrant and it is only if the said Registrant chooses for privacy protection, that the said service shall be offered as a **value added service upon payment of additional charges**. The additional charges shall not be made a part of the default package for registration of domain names.

(ii) Whenever any entity or individual having legitimate interest, law enforcement agencies (LEAs) or the Courts, request for disclosure of data relating to any infringing or unlawful domain name, the following data shall be disclosed by the concerned DNR as soon as possible but not later than 72 hours in terms of the Intermediaries Guidelines 2021:

(a) Name of the Registrant;

(b) Administrative contact;

(c) Technical contact;

(d) Addresses of the above mentioned persons/entities;

(e) Mobile numbers of the above mentioned persons/entities;

(f) Email address of the above mentioned persons/entities;

(g) Any payment related information such as details of credit card, debit card, UPI number, payment platform identities, bank account details, etc., which may be available with the DNR;

(h) Details of any value added services such as hosting of website, brokerage, or any other services offered by the DNR or by Registry concerned.

(iii) If any particular domain name is restrained by an order of injunction or has been found to be used for illegitimate and unlawful purposes, the said domain name shall remain permanently blocked and shall not be put in a common pool in order to disable re-registration of the same very domain name by other DNRs. The appropriate steps in this regard shall be taken by the concerned Registry Operator to ensure that all DNRs having an agreement uniformly give effect to the said direction.

(iv) In the case of trademarks/brands, which are well-known or are invented, arbitrary or fanciful marks, which have attained reputation/goodwill in India, if a Court of Law directs that there would be an injunction on making available the infringing domain name with different extensions or mirror/redirect/alphanumeric variations, the same shall be given effect to by the DNRs and no alternate domain name shall be made available in respect of such brands and marks.

(v) Upon an injunction being issued by the Court in respect of any domain name and the same being communicated to the DNRs, the DNRs shall ensure that no alternative domain name is promoted or being suggested to a prospective Registrant. Any promotion of alternative domain names of an injuncted domain name would disentitle the concerned DNR for safe harbour protection under Section 79 of the IT Act.

(vi) In respect of descriptive and generic marks, the restraining/injunction

orders would be *qua* the specific domain name and any extension of restraining/injunction order for other infringing domain names would be with the intervention of the Joint Registrar before whom the application under Order I Rule 10 of Code of Civil Procedure, 1908 along with affidavit shall be filed and the injunction would be extended. Where any party is aggrieved by the order of the Joint Registrar, the application may be moved or placed before the ld. Single Judge.

(vii) Upon orders being passed by a Court, the infringing domain name shall be transferred to the Plaintiff/trademark owner/brand owner, upon payment of usual charges.

(viii) Search engines and DNRs shall not provide any promotion or marketing or optimization services to infringing and unlawful domain names.

(ix) All DNRs offering services in India shall appoint Grievance Officers within a period of one month from today failing which they would be held as non-compliant DNRs.

(x) Service by email to the respective Grievance Officer's details would be henceforth sufficient service for Court orders and any DNRs who insist upon services through MLAT or through other modes of services shall be held to be non-compliant DNRs.

(xi) In appropriate cases where an entity has repeatedly not complied with orders of the Court, and in the opinion of the Court it is a case where the interest of society at large is being adversely affected, such as cases of frauds, the Court may direct the appropriate authority to block access to the said entity under Section 69A of the Information Technology Act,

2000 read with Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.

(xii) All Registry Operators having valid agreements with ICANN shall take appropriate steps to implement the Trademark Clearing House services and make the same available to all brand owners & registered proprietors of trade marks.

(xiii) All DNRs offering services in India or to customers in India shall undertake verification of Registrant's details at the time of registration and periodic verification of the same. The verification shall be done in terms of KYC requirements mentioned in ***Circular No. 20(3)/2022-CERT-In*** dated 28th April, 2022 issued by Indian Computer Emergency Response Team. This is in line with the NIXI Accreditation Agreement.

(xiv) All DNRs who are enabling registration of domain names which are administered by NIXI as a Registry Operator shall comply and provide requisite registration data to NIXI within one month of this judgment and also update the same on a monthly basis.

(B) ***Directions to the Government***

(xv) The following directions are issued to MeitY, MHA and other relevant Government authorities:

(a) The Government shall hold a stake holder consultation with all DNRs and Registry Operators offering services in India and explore the possibility of putting in place a framework similar to the one used by NIXI by all DNRs for the purpose of domain name registration.

(b) Consider nomination of a nodal agency such as NIXI as the data repository agency for India with which all the Registry Operators and the DNRs would maintain details related to Registrants on a periodic basis so that the said details are made available to the Courts, LEAs and the governmental authorities for the purpose of enforcement of orders of Courts and for preventing misuse. Alternatively, DNRs shall be directed to localize the data in India for easy access. Irrespective of the decision, it is made clear that processing of personal information would be strictly in terms of the DPDP Act and applicable Rules.

(c) In case of a DNR or Registry Operator, which does not comply with the orders of the Courts or with request from LEAs, the offering of services of such DNRs or Registry Operator be blocked by MeitY and DoT under Section 69A of the Information Technology Act, 2000 read with Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.

(d) MeitY along with NIXI shall coordinate with ICANN to enable brand owners in India to avail of TMCH facilities on reasonable terms and conditions so that they can receive notifications whenever any conflicting /infringing domain names are proposed to be registered by any third parties across the globe.

(xvi) The CGPDTM could also consider publishing the list of well-known marks along with the official and authentic website details of the trademark owners so that if any consumer or user wishes to verify the authentic website, the same would be made possible through the website

of the Intellectual Property Office. The same shall also act as sufficient notice to all potential Registrants as to the actual websites of the well-known marks/brands.

(C) ***Directions qua grant of 'Dynamic +' injunction***

(xvii) The Dynamic+ injunction would apply under the following circumstances:

(i) Wherever the brand/trademark appears as it is in the domain name;

(ii) Wherever brand/trademark appears with a prefix or suffix which could lead to confusion;

(iii) Wherever the brand/trademark appears as an alphanumeric variation.

(xvii) Whenever there is a legitimate Registrant who opposes the suspension of the domain name, if the same is communicated by the said Registrant to the concerned DNR, the DNR may then ask the IP owner to obtain a Court order.

(D) ***Directions to Banks***

(xviii) All banks shall mandatorily implement the ***'Beneficiary Bank Account Name Lookup'*** facility in terms of the RBI circular dated 30th December, 2024 for all online payments including payment by UPI through applications such as Google Pay, Paytm, etc.

(xix) All banks shall also abide by the Standard Operating Procedures dated 31st May, 2024 issued by Central Economic Intelligence Bureau for processing and responding to requests received from LEAs.

IX. RELIEFS IN THE SUIT

284. Coming to the facts of this case, in this suit, the Plaintiff prays for protection of trademark '*COLGATE*', '*COLPAL*', and '*COLGATE PALMOLIVE*'. These are registered trademarks. Plaintiffs also enjoy enormous goodwill in these marks. Details of the registrations are set out in the plaint and are not repeated herein for the sake of brevity. The infringing domain names in this case are as under:

285. Initially, an order of *ex-parte* interim injunction was granted on 12th April, 2019 *qua* some of the domain names and the same has been extended to further domain names *vide* orders dated 15th May, 2019, 23rd August, 2019, 27th September, 2019, 24th December, 2019, 20th October, 2023, and 26th June, 2024 as also the corresponding DNRs, banks, etc. However, despite taking steps to implead the respective Registrant in the present suit, none of the Registrants have entered appearance or filed written statements. The Court has also perused the screenshots of the infringing websites placed on record some of which have already been reproduced above and are not being reproduced again for the sake of brevity.

286. In the opinion of the Court, considering the detailed discussion above as also the goodwill and reputation of the Plaintiff, it is clear that the infringing domain names and websites have been used in a manner so as to deceive the general public, as also to entice innocent persons with fake job offers. The fake interview documents, displaying the trade mark and intellectual property of the Plaintiffs, used for defrauding general public have already been extracted above

and the same need not be extracted again.

287. It is the settled position in law that the test for determining whether there has been infringement of the Plaintiff's mark is whether the impugned mark so nearly resembles the mark of Plaintiff that it is likely to deceive or cause confusion in respect of goods for which it is registered.[18]

288. Applying the above tests for infringement in the present case it is clear that the infringing domain names contain the marks of the plaintiff without any alteration, thereby the two are identical, highly likely to deceive the public that the infringing domain names are owned by the Plaintiff. Moreover, the marks of the Plaintiff are extremely distinctive and deserve to be accorded the highest level of protection.

289. Therefore, a ***Dynamic*+ interim injunction** is granted against all the Defendants (Registrants and DNRs) in respect of all seven (7) domain names which are as under:

[18] *Kaviraj Pandit Durga Dutt Sharma v. Navaratna Pharmaceuticals Laboratories*, 1964 SCC OnLine SC 14

Domain Names			
Sr. No.	***Link (do not put https/www)***	***DNR***	***Whether the domain is currently part of the common pool and available for registration? (Yes / No)***
1.	www.colgatepalmoliveindia.in	GoDaddy.com, LLC	No
2.	www.colgatepalmolive.in	GoDaddy.com, LLC	No
3.	www.colpal.in	GoDaddy.com, LLC	No
4.	www.colgateindia.com	CSC Corporate Domains, Inc.	No
5.	www.hrcolgatepalmolive.com	-	Yes
6.	www.colgateindia.in	GoDaddy.com, LLC	No
7.	www.colgatepalmolive.work	GoDaddy.com, LLC	No

290. The injunction shall also extend to any additional or new domain names in the following terms:

> a. *An interim injunction is granted restraining the registrants of all the seven domain names and such other infringing domain names which are discovered during the course of the proceedings as also the persons/entities associated with the said domain names including owners, partners, proprietors, officers, servants, employees, and all others in capacity of principal or agent acting for and on their behalf, or anyone claiming through, by or under them, from using the said infringing domain names for hosting any websites or for undertaking any activities as may result in*

infringement of the Plaintiff's statutory or common law rights in the mark/name/logo '*COLGATE*', '*COLPAL*', '*COLGATE PALMOLIVE*', *and its variants or passing off of such domain names/websites as being connected with the Plaintiff in any manner whatsoever;*

b. *An interim injunction is granted restraining the registrants of all the seven domain names and such other infringing domain names which are discovered during the course of the proceedings as also the persons/entities associated with the said domain names including owners, partners, proprietors, officers, servants, employees, and all others in capacity of principal or agent acting for and on their behalf, or anyone claiming through, by or under it, from, in any manner copying, reproducing, hosting, storing, making available, communicating and publishing or facilitating the same on their websites or on any other websites or online locations owned or operated by them, in any manner whatsoever, imitating the Plaintiffs Website Content amounting to infringement of Plaintiffs copyright therein;*

c. *An interim mandatory injunction is granted directing the DNRs and social media platforms of the seven infringing domain names and such other infringing domain names which are discovered during the course of the proceedings, including their Grievance Officers or anyone acting on their behalf to provide complete disclosure of domain/account information for identification, including name, e-mail, address etc., of person/entity which registered the said account, and suspend access to the domain*

names as also websites operating thereunder. If the websites under the infringing domain names are not being hosted by the DNRs or their related companies, the injunction order shall stand extended to the website hosting companies to take down the websites operating under the infringing domain names;

d. *An order of interim mandatory injunction is issued directing DoT and MeitY to issue a notification calling upon the various internet and telecom service providers registered under it to block access to the websites operating under the infringing domain names or such other websites that may subsequently be notified by the Plaintiff (on Affidavits) to be infringing of its exclusive rights consisting of the mark/name/logo DABUR or any part of the copyrighted content of the Plaintiff's website;*

291. The interim injunctions granted *vide* orders dated 12th, April, 2019, 15th May, 2019, 23rd August, 2019, 27th September, 2019, 24th December, 2019, 20th October, 2023, and 26th June, 2024 are made absolute during the pendency of the present suit, in the above terms.

292. The applications ***I.A. 5399/2019, I.A. 11497/2019, I.A. 18216/2019*** and ***I.A. 31775/2024*** under Order XXXIX Rules 1&2 of CPC are disposed of in the above terms.

X. SUMMARY ADJUDICATION

293. On 31st May, 2025, the present suit along with pending applications was reserved. By way of the above directions, the Court has already disposed of the

applications seeking interim injunction against the infringing domain names. Therefore, the Court shall proceed with considering summary adjudication of the present suit.

294. It is noted that in the present case there is no application by the Plaintiffs seeking summary adjudication of the suit under Order XIII-A of the CPC. However, under Rule 27 of the Delhi High Court Intellectual Property Rights Division Rules, 2022 (hereinafter "*IPD Rules, 2022*") the Court may pass a summary judgement even in the absence of an application to this effect. The Rule 27 of the IPD Rules, 2022 reads as under:

> "***27. Summary Adjudication***
>
> *In cases before the IPD,* ***the Court may pass summary judgment, without the requirement of filing a specific application seeking summary judgment*** *on principles akin to those contained in Order XIIIA, Code of Civil Procedure, 1908 as applicable to commercial suits under the Commercial Courts Act, 2015."*

295. Further, the provisions of the Commercial Courts Act, 2015 read with the Delhi High Court (Original Side) Rules, 2018 (hereinafter "*Original Side Rules, 2018*") would be relevant for consideration in respect of summary adjudication. The Practice Direction 9(h) of the Original Side Rules, 2018 issued pursuant to Section 18 of the Commercial Courts Act, 2018 reads as under:

> *"9.* ***In the case of commercial disputes, the Court may, inter-alia, pass orders as it may think fit for the speedy disposal of the suit or narrowing the controversy between the parties****, including:- […]*
> *h) conduct a Case Management hearing under Order XV-A of the Code and as part of the said case management*

hearing – […]

*ii. **explore the possibility of deciding the dispute by a summary judgment, without a specific application for the said purpose, on the basis of pleadings dispensing with the trial of the suit on the questions of law or of facts on which the parties are not at issue**;"*

296. This Court has in ***Rockwool International A/S & Anr. v. Thermocare Rockwool (India) Pvt. Ltd., 2018:DHC:6774***, considered the necessary conditions for passing summary judgement. A perusal of Order XIII-A Rule 3 of CPC, as amended by the Commercial Courts Act, 2015, reads as under:

"Order XIII-A Summary Judgment
[…]
3. Grounds for summary judgment. – The Court may give a summary judgment against a plaintiff or defendant on a claim if it considers that – (a) the plaintiff has not real prospect of succeeding on the claim or the defendant has no real prospect of successfully defending the claim, as the case may be; and (b) there is no other compelling reason why the claim should not be disposed of before recording of oral evidence."

297. The pre-conditions for passing of a summary judgment under Order XIII-A Rule 3 CPC, as elucidated in ***Rockwool International (supra)*** are:

a) that there is no real prospect of a party succeeding in a claim;

b) that no oral evidence would be required to adjudicate the matter;

c) there is a compelling reason for allowing or disallowing the claim without oral evidence.

298. The ld. Division Bench of this Court in ***Bright Enterprises Pvt. Ltd. v. MJ Bizcraft LLP, 2017:DHC:67-DB,*** laid down principles for granting summary judgments under Order XIII-A of the CPC. The observations of the ld. Division Bench are as follows:

> *"20. Apart from this, we are of the view that the learned Single Judge has gone wrong in invoking the provisions of Order XIIIA CPC for rendering a summary judgment. It is true that Rule 3 of Order XIIIA CPC empowers the Court to give a summary judgment against a plaintiff or defendant on a claim if it considers that – (a) the plaintiff has no real prospect of succeeding on the claim or the defendant has no real prospect of successfully defending the claim, as the case may be; and (b) there is no other compelling reason why the claim should not be disposed of before recording of oral evidence.* ***But, in our view, this power can only be exercised upon an application at any date only after summons have been served on the defendant and not after the Court has framed issues in the suit. In other words, Order XIIIA Rule 2 makes a clear stipulation with regard to the stage for application for summary judgment. The window for summary judgment is after the service of summons on the defendant and prior to the Court framing issues in the suit****. "*

299. In the opinion of this Court, a perusal of the record makes it evident that the concerned domain names have been used in a manner that misleads consumers and infringes upon the Plaintiffs' trademark rights. Further, it is also clear from the detailed analysis hereinabove that the respective Registrants have no valid defence against the contentions of the Plaintiffs. Thus, the summary judgement would be liable to be passed in the present case.

300. However, in order for this Court to exercise the powers of passing summary judgement, it is necessary that all Defendants have been duly served. In the present case there is some doubt as to the status of service to all Defendants.

301. Accordingly, for the purposes of ascertaining the service or for directing fresh service, list before the Joint Registrar on 11th February, 2026 for a report on service.

302. List before the Court on 12th March, 2026. This matter shall be treated as part-heard.

XI. I.A. 15451/2021 (under Order I Rule 10 of CPC)

303. The present application has been filed by GoDaddy.com LLC seeking deletion from the array of parties. However, considering the detailed discussion above and the fact that it is a necessary party in deciding the issues *qua* domain name registration, the present application is dismissed. This dismissal shall however not be construed as an opinion on merits as at this stage this Court is unable to delete GoDaddy for the detailed discussion set out above. The role that GoDaddy has played in respect of each of the infringing domain names and/or websites would have to be looked into to determine whether it has acted purely as an intermediary or not, for which a further in-depth scrutiny would be required.

304. The application is disposed of in the above terms.

PRATHIBA M. SINGH
JUDGE

DECEMBER 24, 2025
dk/kk/msh