



254. 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

255. 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.

256. 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.

257. 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.

258. 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 pyramidal 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.

259. 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.

260. 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.

261. 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.

262. 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.

263. 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.

264. 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.

265. 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.

266. 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.

267. 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.

268. 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.

269. 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.

270. 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.

271. 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.

272. 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.

273. 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.

274. 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 be 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:

275. 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 enjoined 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 Id. 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 PRESENT APPLICATION

276. Coming to the facts of this case, in this suit, the Plaintiff prays for

protection of trademark 'DABUR', , . These are registered trademarks. Plaintiffs also enjoy enormous goodwill in these marks. Details of the registrations are set out in the plaint and not repeated for the sake of brevity.

277. Initially, an order of *ex-parte* interim injunction was granted on 3rd March, 2022 *qua* some of the domain names and the same has been extended to further domain names *vide* orders dated 25th April, 2022 and 15th February, 2025. 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. 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 small businesses which may be enticed into seeking franchisees and distributorships.

278. 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



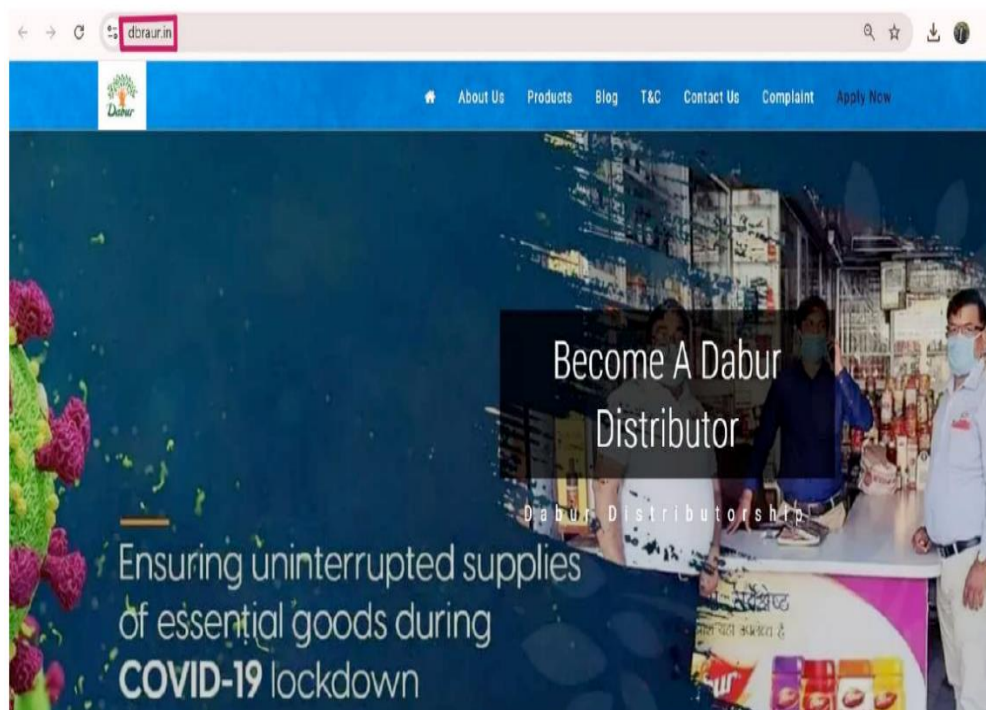
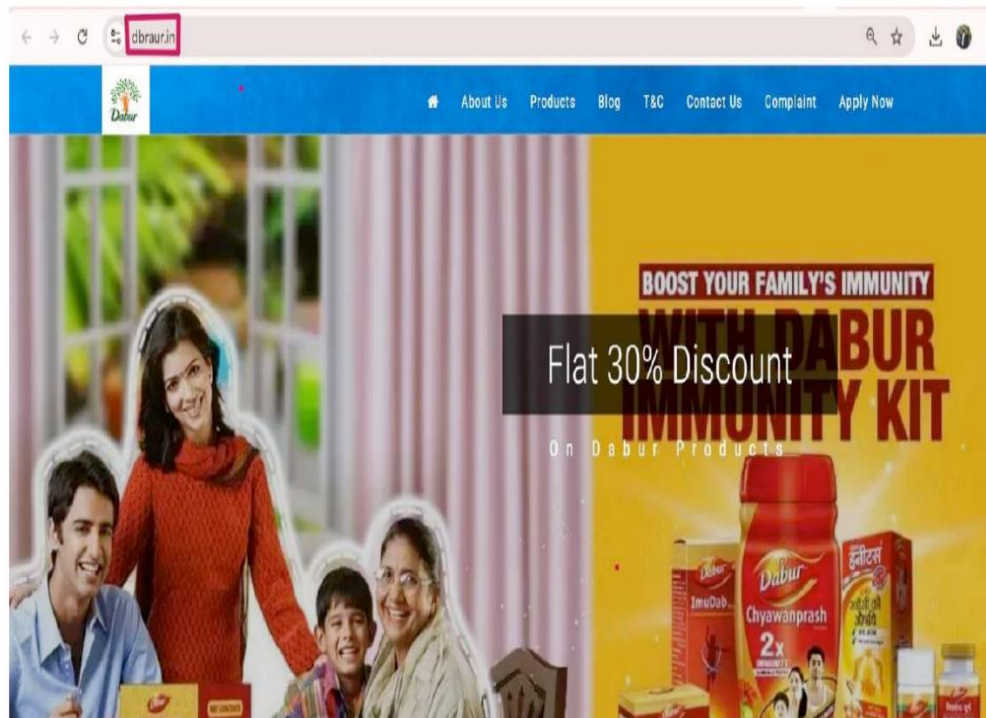
cause confusion in respect of goods for which it is registered.¹⁸

279. Applying the above tests for infringement in the present case it is clear that the infringing domain names barring one (*i.e.*, www.dbraur.in) contain the mark 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. Whereas the domain name www.dbraur.in, is deceptively similar to the mark of the Plaintiff and a perusal of the screenshots of the said website placed on record, leaves no manner of doubt that the same has been registered with the intention to create confusion and deceive the public as to being associated with the Plaintiff. For ease of reference the said screenshots are as under:

¹⁸ *Kaviraj Pandit Durga Dutt Sharma v. Navaratna Pharmaceuticals Laboratories*, 1964 SCC OnLine SC 14



2025:DHC:11862






2025:DHC:11862




← → ↻ dbraur.in/contact-number-dabur-business 🔍 ☆ ⬇️ ⓘ ⋮

Contact us form of Dabur Business


Name*	Mobile*
Email*	Address*
Message*	
<input type="button" value="SUBMIT"/>	




Registered Office
8/3, Asaf Ali Road, New
Delhi-110002



Business Mail
info@daburdistributors.com



Contact Number
(+91) 987-6543-210



280. 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:

Sr. No.	Domain Name	DNR
1.	www.daburdistributor.com	PDR Ltd. d/b/a/- Defendant No.4
2.	www.daburfranchise.in	Godaddy.com LLC - Defendant No. 15
3.	www.daburfranchise.com	Godaddy.com LLC - Defendant No. 15
4.	www.daburdistributorships.in	Hosting Concepts B.V.- Defendant No.5
5.	www.daburfranchisee.in	PDR Ltd. d/b/a/- Defendant No.4
6.	www.daburdistributor.com	Hostinger Operations UAB-Defendant No.16
7.	www.dbraur.in (still active)	Endurance Digital Domain Technology Limited – Defendant



	No.19
--	-------

281. 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 DABUR 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 (through www.dabur.com) 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;*

282. The interim injunctions granted *vide* orders dated 3rd March, 2022, 25th April, 2022 and 15th February, 2025 are made absolute during the pendency



of the present suit, in the above terms.

283. The application is disposed of in the above terms.

X. I.A. 1221/2023

284. The present application has been filed by the Defendant No.15 – GoDaddy.com LLC seeking modification of order dated 1st December, 2022. *Vide* the said order the email details of the counsels for GoDaddy were reproduced in a tabular form. However, inadvertently there is a small typographical error in the said table.

285. The present application has been filed seeking modification of the same as also for placing on record another email which is dedicated for India-related Law Enforcement requests. The said email which is stated to have been in place since 2016 is - IndiaLEInquiries@godaddy.com.

286. For the reasons stated in the application, the same is allowed. The table reproduced in order dated 1st December, 2022 shall now read as under:

Counsel Name	Email ID
Ms. Swati Agarwal	swati.aggarwal@amsshardul.com
Ms. Binsy Susan	binsy.susan@amsshardul.com
Mr. Aashish Somasi	aasish.somasi@amsshardul.com
Nishith Desai Associates	godaddylitigation.nda@nishithdesai.com
Mr. Mrinal Ojha	mrinal.ojha@solarislegal.in
Mr. Debarshi Dutta	debarshi.dutta@solarislegal.in
Mr. Aayush.kevlani	aayush.kevlani@solarislegal.in

287. It is made clear that for all queries by the LEAs for GoDaddy, the email shall be sent at IndiaLEInquiries@godaddy.com as also the respective counsels appearing in the matter from the above mentioned list.

288. Let a copy of this order be communicated to Ms. Hetu Arora Sethi, ASC, GNCTD for necessary information and compliance. Let the Id.



Counsels for GoDaddy appearing in the present application also communicate this order to Ms. Sethi for necessary information and compliance.

289. The application is disposed of in the above terms.

XI. I.A. 8588/2025

290. The present application has been filed by Defendant No. 17 – Meta Platforms Inc., seeking modification/clarification of order dated 15th February, 2025 *vide* which the Court had impleaded the applicant in the present suit and extended the order dated 3rd March, 2022 to the applicant. The operative portion of the said order reads:

“3. The Plaintiff prays for impleadment of the domain name/ website -

https://www.daburdistributorships.in/index.html and https://daburdistributor.com. On the said websites, various images of the Plaintiff’s products including the screenshots of the Plaintiff’s website have been uploaded and the said domain names/websites are passing off as being connected with the Plaintiff.

4. Ld. Counsel for the Plaintiff submits that there is also clear violation of the copyright of the Plaintiff by the said websites.

5. The said domain names are stated to have been registered by Hostinger Operations UAB and the website is also being promoted on Facebook, X (previously known as Twitter) and Instagram.

6. In view of the averments made in the present application, the same is allowed.

7. The domain name registrar - Hostinger Operations UAB, Meta Platforms and X Crop. are impleaded as Defendant Nos. 16, 17 and 18.

8. The order dated 3rd March, 2022 as modified on 25th April, 2022 shall now stand extend to all these Defendants as well.

9. Ld. Counsel appearing for the Meta Platforms/Defendant No.17 be furnished a copy of the



entire suit papers along with all the applications.

10. The newly impleaded Defendants shall be served through the respective Grievance Officers.”

291. It is stated that the directions passed in order dated 3rd March, 2022 in respect of taking down of infringing domain names cannot be complied with by the applicant and that the same would be in the hands of the Domain Name Registrar or the Internet Service Providers. Thus, the prayer is to clarify and limit the directions in respect of the applicant.

292. It is submitted on behalf of the Plaintiff that a similar clarification was also sought by M/s. Hosting Concepts BV (hereinafter “*Hosting Concepts*”) in **I.A. 9363/2022** which was dismissed *vide* order dated 27th February, 2024.

293. The Court has heard the parties and perused the documents on record. On 27th February, 2024, the Court had considered an application for modification of the order dated 3rd March, 2022. The relevant portion of the said order reads as under:

“6. This is an application moved on behalf of the Defendant No.5 seeking modification of the order dated 3rd March, 2022 read with order dated 25th April, 2022. It is submitted by Ms. Geetanjali Vishwanathan, ld. Counsel, that the Joint Registrar ought to look into the domain names complained against carefully and pass an order rather than take down being effected, merely upon information being given by the Plaintiff. It is urged by her that mere filing of an affidavit by the Plaintiff is not a sufficient cause for the Defendant being forced to lock/block the domain name. It is prayed by Defendant No.5 in the application that the Plaintiff, upon coming across any domain names that it finds to be infringing, must file an affidavit or application before this Court pointing out such domain names, and require the Defendant No. 5 to lock/block such domain names



and maintain status quo only after a court order specifically finding such domain names to be infringing.

7. The Court has repeatedly heard these matters. Considering the nature of the mark 'DABUR', which is an inventive mark, the Court is not inclined to modify the order dated 25th April, 2022. If, however, the Defendant No.5 has any concern with a particular domain name which could be of a genuine user, it may inform the Plaintiff of the same, in which case, the Plaintiff may move an application before this Court in respect of the said domain name."

294. Considering the order dated 27th March, 2024 and the judgement passed hereunder, the Court is not inclined to modify the order dated 15th February, 2025.

295. The application is disposed of in the above terms.

CS(COMM) 135/2022

296. List before the Roster Bench of the IPD, for further proceedings on 28th January, 2026.

**PRATHIBA M. SINGH
JUDGE**

DECEMBER 24, 2025
dk/kk/msh