INDIALAW

COMMERCIAL/CORPORATE | INTELLECTUAL PROPERTY RIGHTS

The Delhi High Court Judgement On Domain Name Fraud: An Analysis Of Dabur India Limited V. Ashok Kumar

AUTHOR Dinesh Gupta, Ishika Soni

PUBLISHED 9 January 2026

Introduction

In a significant ruling aimed at curbing online domain name fraud, the Delhi High Court in the case of Dabur India Limited v. Ashok Kumar has directed a mandatory e-KYC verification of domain name registrants, holding that weak identity verification mechanisms have enabled the rise of phishing websites and digital impersonation. The case exposed an ecosystem where deceptive domain names, cloned websites, and impersonation portals operate at scale, targeting both brand owners and the general public. These fraudulent operations often disappear and resurface under new domain names faster than conventional legal remedies can restrain them.

Justice Pratibha M Singh observed and addresses the structural weaknesses that allow such fraud to thrive where fraudsters register domain names closely resembling well-known brands, create convincing websites, and project themselves as authorised distributors, franchise partners, recruiters, or investment facilitators. Members of the public are persuaded to deposit “registration fees”, “processing fees”, or “security amounts”, after which the websites vanish. The ruling recognises that digital fraud is no longer episodic or isolated, but organised and repeatable.

The registrant details are frequently false, masked, or hidden behind proxy services. By the time a complaint is made or a court order is passed, the operator have already migrated to a new domain name, often with minor spelling variations or different extensions. This repetitive cycle renders traditional injunctions ineffective.

Table of contents

- Introduction
- Factual Background
- Legal issues Raised
- Judicial Reasoning
- Court’s Order & Directions
  - Direction to Domain Name Registrars & Registry Operators
  - Directions to Government Authorities
  - Directions to Banking Sector
  - Other Directions
- Conclusion
- Author’s View

Factual Background

The present case arose from a disturbing pattern of cyber fraud where unknown individuals registered domain names incorporating the well-known trademark “DABUR”. The civil suit instituted by Dabur India Limited, a well-known Indian company with extensive goodwill and reputation in the fast-moving consumer goods sector. Dabur is the proprietor of the registered trademark “DABUR” and holds copyright in the artistic works comprising the labels, packaging, trade dress, and overall get-up of its products. The brand enjoys widespread recognition across India and internationally, and its trademarks have been in continuous use for several decades.

The suit was filed under Section 20 of the Code of Civil Procedure, 1908, read with Section 27 of the Trademark Act, 1999, seeking, inter alia, permanent injunction, damages, and other consequential reliefs in respect of infringement of its intellectual property rights, passing off, and unfair competition. Dabur alleged that unknown individuals had registered and were operating multiple domain names incorporating the “Dabur” mark, without authorisation, and were using such domain names to host websites that falsely projected an association with the plaintiff.

These fraudulent domain names were being systematically exploited to deceive innocent members of the public through various schemes by impersonating “DABUR” and its word mark and represented themselves as official platforms of the company. They invited members of the public to apply for distributorship, franchise opportunities, and agency appointments for the sale of Dabur products.

At the time of instituting of suits Dabur identified seven infringing domain names. One of these websites explicitly demanded payment of approximately Rs. 25,000 from prospective distributors or franchisees as a registration or processing fee. The plaintiff further pointed out that these activities were not isolated incidents but formed part of a recurring pattern. The gravity of the situation was increased by the fact that the details of the infringing domain names were systematically masked by the Domain Name Registrars (DNRs) using “privacy protect” features, preventing plaintiffs from initiating proceedings against the actual perpetuators.

During the course of proceedings, the Court was informed that similar suits has been filed by other well-known corporate entities also who are facing similar or same forms of digital impersonation to deceive the public including Amul, Meesho, Colgate, ITC, and Mont Blanc, etc., all facing similar fraudulent domain name registrations. The Court took note of the fact that, across cases, more than 1,100 infringing domain names had been identified, yet almost no registrant has come forward to claim any legitimate interest or defend their conduct. The Court noted that the scale of the fraud needs a coordinated investigation and broad remedial measures.

Legal issues Raised

1. Whether Domain Name Registrars are under a legal obligation to prevent registration of infringing and fraudulent domain names and whether the existing domain name registration practices are adequate to protect trademark rights?
2. What measures may be directed by the Court to the Domain Name Registrars and Registry Operators to safeguard the trademark rights under the Trademark Act, 1999?
3. What are the obligations and liabilities of Domain Name Registrars in respect of alleged infringing domain names, and whether these obligations are sufficient for protecting intellectual property rights of third parties?

Judicial Reasoning

Justice Pratibha M Singh held that the misuse of domain names in the present cases went far beyond the isolated instances of trademark infringement and reflected a systematic pattern of online fraud and consumer deception. The Court recognized that domain names function as a key indicator of commercial origin in the digital space and that deceptively similar domain names, when combined with cloned content and use of well-known trademarks, are capable of misleading the public at large and causing immediate harm. In view of the speed, anonymity, and scale at which such activities occur, the court found that traditional, domain-specific injunctions were inadequate to address the problem effectively.

Court’s Order & Directions

After examining the scale and recurring nature of the fraud placed before it, the Delhi High Court issued a detailed set of directions intended to introduce accountability and traceability into the domain name registration ecosystem. The Court made it very clear that the isolated injunctions against individual websites would not suffice when the very structure of domain registration enables the repeated abuses.

Direction to Domain Name Registrars & Registry Operators

- The Court mandated compulsory Electronic Know Your Customer (e-KYC) verification for all domain name registrants, both at the time of registration and through periodic re-verification. Domain Name Registrars (DNRs) were directed to collect accurate, authentic, and verifiable identity information.
- DNRs to maintain complete technical and transactional records relating to domain registrations including IP addresses, timestamps, login histories etc.
- The Court directed that registrant information and technical data must be furnished within 72 hours whenever formally sought by courts, law enforcement agencies, or legitimate right holders.
- Upon 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 suggested to a prospective Registrant. Any promotion of alternative domain names of an injuncted domain name would disentitle the concerned DNR for the safe harbour protection under Section 79 of the IT Act.
- Restrained the DNRs from offering privacy or identity-masking services by default. Such protection may only be extended where it is specifically requested by the registrant and only after full compliance with e-KYC and verification requirements.

- All DNRs enabling registration of domain names administered by NIXI must provide requisite registration data to NIXI within 1 month.
- Registry Operators were directed to implement technical measures to prevent recycling or re-registration of infringing domain names.

Directions to Government Authorities

- The Court directed the Government to hold stakeholder consultations with DNRs and Registry Operators to examine the framework same followed by NIXI.
- 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 the Registrants on a periodic basis.
- MeitY along with NIXI shall coordinate with the ICANN to enable the 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 other third party.
- The non-compliant DNRs or Registry Operators may be blocked by MeitY and DOT under Section 69A of the Information Technology Act, 2000.

Directions to Banking Sector

The Court also addressed vulnerabilities within the banking system that enabled fraudsters to receive payments by impersonating well-known brands.

- All banks shall mandatorily implement the “Beneficiary Bank Account Name Lookup” facility in terms of the RBI Circular dated 30th December, 2024 for all the online payments. Pursuant to the Court directions, the Reserve Bank of India (RBI) introduced the “Beneficiary Bank Account Name Lookup” facility for RTGS and NEFT systems. This mechanism allows remitters to verify the name of the bank account holder before initiating a transfer, thereby reducing the risk of mistaken or fraudulent payments.
- All banks were directed to implement this facility without any charge to customers by 2025.
- All banks shall also abide by the Standard Operating Procedures dated 31st May, 2024 issued by Central Economics Intelligence Bureau for processing and responding to requests received from LEAs.

Other Directions

- The CGPDTM may consider publishing a consolidated list of all registered well-known trademarks, along with the official and authenticated website details of the respective trademark owners, to enable consumers and users to verify such information directly through the Intellectual Property Office’s website.
- All DNRs offering services in India shall appoint a Grievance Officers within a period of one month from the judgment date failing which they would be held as non-complaint DNRs.
- Search engines & DNRs shall not provide any promotion or marketing or optimization services to infringing and unlawful domain names.

Accordingly, in the present case, the Court granted the injunctions against the identified infringing domain names and extended protection to future deceptive variants through a dynamic plus injunction, (a relief which permits plaintiffs to implead mirror, redirect, and variations of infringing domain named under Order I Rule 10 of the Code of Civil Procedure, without being compelled to institute fresh suits each time a new variant appears), ensuring plaintiff is not forced into repetitive litigation to curb recurring fraud.

Conclusion

The judgment in Dabur India limited v. Ashok Kumar marks a shift from reactive adjudication to preventive regulation. By addressing the structural weaknesses in the domain registration ecosystem, the Delhi High Court has attempted to curb the churn-and-replace model that allows fraud to flourish online. The ruling strengthens enforcement for rights holders while offering greater protection to consumers navigating digital marketplace.

Author’s View

The judgment recognises that online fraud linked to domain names is not incidental but structural in nature. Rather than treating domain name misuse as a series of disconnected trademark violations, the Court has recognised it as an organised and repeatable abuse of systematic gaps within the online registration framework. By shifting attention to the point of entry, domain

registration itself, the Court has addressed the problem at its source rather than merely responding to its consequences. The decision clarifies that intermediary protection cannot exist without meaningful diligence and accountability.

For more details, write to us at: contact@indialaw.in

References:

- CS (COMM) 135/2022 and I.As. 3423/2022, 1221/2023 and 8858/2025
- https://delhihighcourt.nic.in/app/showFileJudgment/PMS24122025SC1352022_193906.pdf

Related Practice Areas

Intellectual Property Rights (IPR) **Corporate & Commercial**