Landmark ruling on domain name fraud and systemic reforms in digital commerce

News & Updates • January 2, 2026

First published by Lexology.

By: Pravin Anand, Saif Khan and Shobhit Agrawal

On 24th December, 2025, Delhi High Court delivered a groundbreaking judgment in *Colgate Palmolive Company & Anr. v. NIXI & Anr.* (CS(COMM) 193/2019), addressing the rampant misuse of well-known trademarks through fraudulent domain name registrations. Hon'ble Ms. Justice Prathiba M. Singh in this landmark decision provides a comprehensive systemic reform to protect intellectual property rights and public interest in the digital age.

A. Background

- The case emerged from a disturbing pattern of cyber fraud where unknown individuals registered domain names incorporating the well-known trademarks 'COLGATE', 'COLPAL', and 'COLGATE PALMOLIVE'. These fraudulent domain names were being systematically exploited to deceive innocent members of the public through various schemes, including fake job offers, fraudulent franchise opportunities, and distributorship schemes. The *modus operandi* was particularly insidious: registrants would create websites hosting almost identical content to the plaintiffs' official website, use similar logos and marks, and provide misleading information to entice the general public into making payments through digital transactions to bank accounts completely unconnected to the plaintiffs. In one instance, an individual using the name Vishal Sharma fraudulently portrayed himself as the head of the Human Resources Department and solicited money from targeted persons for fake interviews using the domain name 'colgatepalmoliveindia.in'.
- The gravity of the situation was compounded by the fact that the WHOIS details of infringing domain names were systematically masked by Domain Name Registrars (DNRs) using "privacy protect" features, preventing plaintiffs from initiating proceedings against the actual perpetrators.
- The case was part of a larger batch of matters involving multiple well-known brands including Tata Sky, Amul, Bajaj Finance, Dabur, Meesho, Croma, ITC, and Mont Blanc, all facing similar fraudulent domain name registrations. The Court recognized that these were not isolated incidents but systemic problems requiring consolidated investigation and comprehensive remedies. Investigation by the Intellectual Fusion and Strategic Operations (IFSO) unit of Delhi Police revealed that crores of rupees had been fraudulently collected from innocent persons duped by these infringing domain

names. The scale of the fraud was staggering, with status reports indicating illegal collection of substantial amounts under the garb of offering distributorships, franchises, and employment.

B. Legal Issues Addressed

- The Court framed three critical issues for adjudication:
- What are the obligations and liabilities of DNRs in respect of alleged infringing domain names, and whether these obligations are sufficient for protecting intellectual property rights of third parties?
- What measures may be directed by the Court to be implemented by DNRs and Registry Operators to safeguard trademark rights?
- What measures may be directed against DNRs who refuse to comply with Court orders?
- One of the most significant obstacles identified by the Court was the widespread abuse of "privacy protect" features offered by DNRs. While ostensibly designed to protect legitimate privacy interests, these features were being exploited to enable fraudsters to register infringing domain names in complete anonymity. The Court found that DNRs were providing privacy protection as a default "opt-out" system, thereby masking the identities of registrants even from trademark owners. Most registration details were either fictitious, wholly incorrect, or impossible to trace. This systematic anonymization enabled the entire gamut of fraudulent transactions and cyber fraud to be committed merely by registering infringing domain names and hosting misleading websites.
- A particularly troubling aspect of the case was the brazen non-compliance by several foreign DNRs with Indian Court orders. DNRs including Namecheap Inc., Dynadot LLC, and Tucows Inc. initially refused to comply with Court directions. Namecheap Inc. specifically took the position that Indian Court orders were not "government orders" and that they were not required to comply with foreign Court orders. Only after the Court issued blocking orders against these non-compliant DNRs did they finally agree to implement the Court's directions. This demonstrated that without coercive measures, there was no effective mechanism to ensure compliance.

C. Directions passed by the Court

- The judgment goes far beyond traditional trademark litigation to order comprehensive systemic reforms addressing multiple stakeholders:
- *Directions to DNRs and Registry Operators:* The Court directed that DNRs shall not mask details of registrants on a default "opt-out" basis; privacy protection should only be provided if specifically chosen by the registrant. All DNRs enabling registration of domain names administered by NIXI must provide requisite registration data to NIXI within one month. DNRs must appoint Grievance Officers, and service by email to these officers shall constitute sufficient service for Court orders. DNRs insisting on MLAT (Mutual Legal Assistance Treaty) or other modes of service shall be held non-compliant.
- *Directions to Government Authorities*: The Court directed the Government to hold stakeholder consultations with DNRs and Registry Operators to explore a framework similar to that used by

NIXI. The Government must consider nominating NIXI as a data repository agency for India, with which all Registry Operators and DNRs would maintain registrant details on a periodic basis, or alternatively, DNRs shall localize data in India. Most significantly, the Court held that non-compliant DNRs or Registry Operators may be blocked by MeitY and DoT under Section 69A of the IT Act, 2000.

- *Banking Sector Reforms*:The judgment addressed crucial gaps in the banking system that facilitated fraud. The Court noted that fraudsters could receive payments because innocent persons making payments did not realize they were not paying the actual brand owners. Pursuant to Court directions, the Reserve Bank of India introduced the 'Beneficiary Bank Account Name Lookup' facility for RTGS and NEFT systems on 30th December, 2024. This allows remitters to verify the name of the bank account to which money is being transferred before initiating the transfer, thereby preventing mistakes and frauds. All banks were mandated to implement this facility without any charge to customers by 1st April, 2025. The Court also directed all banks to abide by the Standard Operating Procedures issued by the Central Economic Intelligence Bureau for processing and responding to requests from Law Enforcement Agencies.

D. Dynamic+ Injunctions

The judgment represents a watershed moment in Indian intellectual property jurisprudence and cyber law. By addressing not just the immediate infringement but the entire ecosystem enabling domain name fraud—from DNR practices to banking systems to law enforcement coordination—Justice Singh's comprehensive ruling provides a blueprint for protecting both trademark rights and public interest in the digital age. The judgment's requirement for data localization, privacy protect reforms, beneficiary account verification, and coercive measures against non-compliant DNRs creates a robust framework that other jurisdictions may well seek to emulate. Most importantly, it recognizes that in an era where e-commerce and digital identity are paramount, traditional legal remedies must evolve to meet new challenges, and courts must take a holistic, systemic approach to ensure justice and protect vulnerable consumers from sophisticated cyber frauds masquerading behind legitimate trademarks.

Building upon the jurisprudence established in *UTV Software Communication Ltd. v. 1337X.To*, the Court granted a "Dynamic+" injunction. This innovative remedy allows plaintiffs to implead mirror, redirect, and alphanumeric variations of infringing domain names under Order I Rule 10 of the CPC without filing fresh suits. The Court reaffirmed the fundamental principle established in *Satyam Infoway Ltd. v. Siffynet Solutions (P) Ltd.* that domain names are recognized as worthy of trademark protection. It held that the use of well-known marks, brands, and logos as domain names constitutes infringement of plaintiffs' statutory rights as well as common law rights. The judgment emphasized that registration of an infringing domain name itself constitutes a violation of rights, rejecting arguments that actual use is required before infringement can be found.

Significantly, the Court recognized that this case transcended mere private intellectual property protection. The judgment held that courts have a larger duty to the general public to ensure that misuse of domain names for offering jobs, dealerships, franchises, and collecting monies under fraudulent pretenses is eliminated as much as possible. The Court noted that apart from violating plaintiffs' intellectual property rights, there was a larger public interest being affected, as innocent members of the public were being duped and conned into believing that activities run under these domain names were being offered by the actual brand owners.

KEY CONTACTS

Pravin Anand
Managing Partner
View Bio of Pravin Anand

Saif Khan
Partner
View Bio of Saif Khan

Shobhit Agrawal
Associate Partner
View Bio of Shobhit Agrawal