India's domain KYC rulings: Ending anonymity in online fraud

News & Updates • February 18, 2026

'First published on India Business Law Journal'

By: Madhu Rewari

As cyber fraud and digital impersonation spreads, India may have a solution to the anonymity that allows so many scammers to practise their deceptions unhindered.

In the recent case of *Colgate Palmolive Company and Anr v NIXI and Anr*, Delhi High Court circumvented the frustrating game of "whack-a-mole" and addressed the anonymity that allows online fraud to flourish. Protecting major brands such as Colgate, Dabur and Bajaj Finance, its order established a bold framework. This requires domain registrants to follow stringent know-your-customer (KYC) norms and holds domain name registrars (DNR) responsible by revoking their safe harbour immunity for failing to prevent abuse.

India court mandates domain KYC

The court set out in detail how cybercrime works. Fraudsters register a domain name that mimics a well-known brand, such as colgate-jobs.com. The registrant's identity is shielded by the default privacy protection features offered by DNRs such as GoDaddy. Their details are fictitious, with fake addresses and temporary phone numbers.

These domains become "engines for large scale deception". Fake websites are set up, offering non-existent jobs, dealerships and franchises and inveigling the public into paying into fraudulent accounts. When the brand owner or law enforcement act, money and perpetrators are long gone. The court found that fraudulent collections attract tens of millions of rupees.

Global DNRs collect the least amount of data. However, following the example of regulatory frameworks such as the EU's GDPR, the court directed that DNRs offering services in India must verify registrants' identities. This follows the e-KYC norms adopted by the National Internet Exchange of India (NIXI) for national, or .in, domains. DNRs must collect and verify details such as names, addresses, emails and phone numbers through authenticated means.

DNRs lose safe harbour protection

The court held that the safe-harbour provisions of section 79 of the Information Technology Act, 2000 (act) protect only genuine, passive intermediaries, not platforms that facilitate unlawful activity. Registrars suggest and promote alternative infringing domain names, sell at exorbitant prices "premium" domains containing well-known trademarks and offer web hosting and marketing services that abet fraudulent sites.

Such services not only generate revenue for DNRs but also help those with illegal and unlawful motives to register domain names similar to well-known marks and brands. These DNRs are not mere intermediaries but are complicit in the infringement. The judgment means that any DNR promoting alternative versions of an already injuncted domain name will lose its safe harbour protection and will be an infringer itself, liable for damages.

The court warned non-compliant DNRs that refusing to comply with court orders, for example by insisting on a subpoena from a foreign court, will see their services blocked under section 69A of the act. Defiance that enables widespread fraud, changes a civil dispute to a matter of public order, impinging on the country's sovereignty.

India tightens registrar KYC rules

The comprehensive order directs DNRs to end the default masking of registrant details, making privacy protection a paid opt-in service. They must carry out KYC verification for all registrants in India. They must disclose all registrant information within 72 hours of a court or law enforcement request. DNRs must appoint India-based grievance officers and accept court orders by email. They will lose their safe harbour protection if they promote infringing domain alternatives. The government may block them completely for repeated non-compliance. Infringing domains have to be permanently blocked and transferred to the rightful trademark owner, while DNRs are prohibited from making available variations of well-known marks. The government has to consider setting up a centralised data repository and co-ordinating with international regulator, ICANN, to make brand protection services more accessible.

By introducing measures such as the Dynamic+ injunction that automatically extends protection to future infringing domains and requiring banks to implement a beneficiary name lookup facility to prevent payment fraud, courts have created a holistic, multi-pronged solution.

India offers a robust and effective framework. Digital access comes with digital responsibility and the age of profiting from unaccountable anonymity is over.

KEY CONTACT

Madhu Rewari

Partner

View Bio of Madhu Rewari