Where Does Liability Lie in Domain Name Infringement?

Thought Leadership • March 8, 2021

This article about cybersquatting and WHOIS anonymity was first published in the 8th March 2021 edition of the Asia Business Law Journal. **Author: Saif Khan** Since the advent of the internet, a domain name has practically served as the first point of contact for a potential customer of any business. A domain name can be registered by anyone upon payment of the applicable fee, and furnishing basic contact information, as a part of the domain's Whois database. This process has been on first come, first served basis, with no real responsibility on anyone towards legitimacy of allotment of a particular domain to an applicant. Consequently, it has always been easy for anyone to indulge in cybersquatting. The Whois database is a listing of all registered domains, and its management is administered by the Internet Corporation for Assigned Names and Numbers (ICANN). It is intended to make the information about websites and their owners accessible, so as to enable resolution of disputes relating to them. However, the lack of any sanctity, legal obligation, or even a basic gatekeeping of the contact information furnished by the domain registrant, enable squatting or infringing domain names to be extremely easy. As a result, the Whois database becomes meaningless in most cases of dishonest domain registrations, as it fails to identify the actual registrant of an unscrupulous domain, thereby disabling right owners from taking legal remedies. The common menace by domain squatters is that they register domains of a known brand, with some combinations, and send out bulk emails to targeted sets of people, inducing them to part with money. Such a modus operandi has also come to light in actions taken by law enforcement against fake call centres, where the fraudsters were found to use domains and sub-domains created with combinations of names of a famous software company to offer fraudulent tech support services online to people outside India. At the time of writing this article, Delhi High Court is seized with litigations by brand owners complaining of registrations of series of infringing domain names, which are used for fraud. The common pattern in all such cases is that the identity of the domain registrant is unknown for being false and/or hidden. Consequently, there remains no option for a plaintiff but to necessarily array the domain registrar(s) as a defendant in the suit, which claims the safe harbour of intermediary in such actions and escapes any other liability, apart from blocking the domains complained of. The domain registrars also resist injunctions against future issuance of domain names under a particular trademark, taking a common stand that, firstly, the transaction is not in their control for being an automated process, and secondly, that it is impossible for domain registrars to monitor each domain in a space spanning millions of domains. Furthermore, the domain registrars assert that they are neither an appropriate entity nor equipped to decide whether a particular domain causes an infringement of someone's trademark rights. While each of the above-mentioned standpoints can be fairly understood and conceded to, in the view of the authors the crux of the issue revolves at the registrar's disinclination to perform a basic mandatory due diligence as to the identity

of the domain registrants, or what is commonly termed as know your customer (KYC) record. It cannot be denied that the registrars offer their services of registration of domain for profit, as well as that the scope of misuse of a domain name is vast, in both extent and territorial reach. Therefore, a proper due diligence towards identity of a domain registrant is an imminent need of the hour and a complete absence of it by the registrars is surprising. Hence, mandating the domain registrar with the task of securing a basic KYC record of each domain registrant to begin with shall significantly reduce the time in identifying cybersquatters. Such a practice also secures the interests of domain registrars, as the right holders can then go after the real culprits without necessarily dragging domain registrars into legal actions. The national domain management authorities must also take the initiative to frame policies so that the domains under their jurisdiction are issued in compliance with strict KYC requirements. This is especially imperative due to the repeated stand taken by the domain registrars that they are not mandated by any law or rule to conduct any KYC due diligence for domain registrations. There exists an imminent need for all stakeholders to collaborate and come up with a domain name framework that ensures that private rights and public interests are secured. If steps are not taken by stakeholders, there could be a serious problem for courts and law enforcement to deal with the huge number of cases, as the real victims are almost always the innocent general public.