CONTRIBUTOR

G&W Legal

ARTICLE

India: Is That You, Jim? : Scams Involving Trade Marks / IP

05 July 2023

by Manavi Jain , Arjun Khurana and Dishti Titus

G&W Legal

This is the digital era: there is no denying that the world is ruled by technology and the internet today. While the laws are trying their best to stay current (.in some cases, catch up!) with the changing world and its technological advancements, the 'dark side' of technology has given rise to rather creative forms of illegal activities. Here, we have discussed the issues surrounding brand / trademark misuse and infringement in the digital age - specifically in relation to online frauds and scams. It's not all doom and gloom, though: we have added some recommendations on preventive best practices as well as available options to deal with such violations (.if you found this article *after* the prevention window expired!).

But first....

Before we delve into the actual analysis and discussion, a quick roadmap that'll help you gain some context. The internet is called the 'web' for a reason - the way things are interconnected across this web translates into a similar entanglement of legal issues as well. The underlying issue for digital violations would perhaps, in many cases, be some form of data / privacy violation - but we're not going to be dealing with that aspect in detail in this article. We'll still be touching on this (and other incidental legal issues) to the extent they overlap with the main topic of this piece - misuse of brands in online scams and frauds.

How are Brands (Mis)Used in Online Scams and Frauds

From a brand's perspective, the core of online scams or frauds is very similar to that of 'traditional' brand violations - if we can call them that. Brand owners acquire the trust and confidence of the consuming public over the course of time - although the definition of 'course of time' in itself is now evolving.[1] Acts of misuse / infringement of a brand are usually derived out of an exploitation of the trust and the confidence the consuming public reposes in a brand.[2]

The scale at which digital brand violations are, or potentially can be, perpetrated is what makes these relevant and distinguishable. Further, the element of 'repute' of a brand is perhaps more at play in such violations; the higher the repute of a brand, the higher the chances of it being misused in digital violations. Another distinguishable feature of such scams is the difficulty in enforcing against bad actors / infringing parties because they 'reside' (so to speak) in the ethers of the web - zeroing down their identities or the physical location of their operations is almost a Sisyphean task. Further, the 'hydra'-like (we promise this is the last mythological reference we've used.in this paragraph) tendencies of these bad actors to regenerate and relapse into the infringing activities, even if one avenue of it is legally slain, makes any real enforcement effort even more gruelling and challenging.

The ingredients above are at play in multiple ways in cases concerning digital brand violations - some common types of such violations are listed below[3]:

i. **Domain Spoofing & Cybersquatting (*Using Brand Names in Fraudulent Domain Names*)**: One of the most common frauds online is for scammers to incorporate - within a domain name - a well-known / reputed trademark completely, or a deceptively or confusingly similar variant thereof. The domain name itself is then either 'parked' with an inactive website (and often with web-links to competing businesses) - often used by scammers to extort money from genuine brand owners - and / or used as a part of e-mail IDs to defraud consumers.

goodwill of popular brands. Scammers may create a fake digital identity, using a genuine brand's IP to lend themselves the veneer of credibility, and contact unwitting individuals with fictitious job vacancies. These are propagated through email IDs hosted on the deceptively similar domain names discussed above, and innocent candidates are often duped into transferring money or disclosing personal information on the pretext of 'background checks', 'training' etc. Once the money or data changes hands, the fake digital identity is often destroyed (or made dormant) to avoid a trace-back.

ii. **Fraudulent Websites**: This is usually something done in addition to the first type discussed above, where the scammers create a 'fake' website - often retaining the basic elements or look-and-feel of the genuine brand-owner's website but populating it with fake contact information and the like. However, sometimes, websites containing a similar look-and-feel and misusing brands / trademarks can be hosted even when the domain name is not deceptively similar to or incorporates the said brands / trademarks. This is often seen in relation to service / repair websites for electronic goods - where scammers would use a single website with an unrelated domain name and misuse the brands of multiple owners (for instance, a domain name computerrepairs.in to offer repair services for multiple brands like Dell, Lenovo, etc.). Here, the scammers sometimes (..yes sometimes, not always) use an inconspicuous disclaimer stating they are not an authorized repair centre - which is bound to go unnoticed by a consumer (or so they hope - and they're not entirely wrong). The descriptions, photos, text, etc. used on the fraudulent website are usually lifted directly from genuine brand owners' websites. The scammers could also use meta-tagging to help increase the visibility of their fraudulent website to consumers looking up the internet for the same, and/or incorrectly claim to be 'authorized' parties./computerrepairs.in

iii. **Textual / Verbal Impersonations**: Scammers reach out to consumers, misrepresenting themselves as an official / employee of a bank or any e-commerce platform for instance, with tempting offers - and deceive consumers into paying them anything ranging from small to significant sums of money.

iv. **Fraudulent Mobile Applications**: This one is often seen in relation to brands and trademarks used for banking / financial goods / services. Here, the scammers create a fraudulent mobile application under reputed brands and trademarks.

Whodunnit? Question of Liability

Stating the obvious here, but unless the brand owners are in some way responsible or were a conduit for the scam / fraud committed, they should not incur any legal liability. That said, often aggrieved consumers turn to the brand owners seeking recourse owing to the inherent nature of these scams - sometimes under the misplaced belief that the brand had some role to play in it - without realizing that the brand owners were as in the dark about things as they themselves were.

Compliances

While there is no directly flowing liability incurred by the brand owners in such cases, there might be a few compliance-based responsibilities placed on them, failing to comply with which, the brand owners may incur liability in a more indirect manner. For instance, under the Directions issued by the Indian Computer Emergency Response Team (CERT-In) in 2022[4], there is a requirement for 'timely' reporting of certain types of cybercrimes. CERT-In Directions are relatively new and have not been interpreted sufficiently for the scope to be tested out yet, but these do cover some reporting compliances, particularly for phishing scams as well as scams perpetrated under a 'fake' mobile app.[5] Similar requirements - mostly for compliances, but in some cases (again, depending on the role - or lack thereof - of the brand owner) even liability - are contained in the (many) Directions and Guidelines issued by the Reserve Bank of India, Securities and Exchange Board of India[6], etc. from time to time.

Legal Actions: Smoking Gun Violation or Inconclusive?

With the proliferation of scams especially in the current social media-led environment, the biggest risk-exposure for brands (that have been misused) is perhaps in the realm of PR and optics. This is why the first reaction of brands (being misused) is often a public statement distancing the brand from the fraud being perpetuated - which is not merely to avoid liability but also to put forth a consumer-first approach. Crisis comms are crucial to get right, and this is where a company's corporate comms team often plays a critical role.

Outside of this, in cases where digital brand violations have already taken place, brand owners have the option to pursue legal actions (civil or criminal) as well as alternative dispute resolution options. How effective these options are will depend on many factors, but as long as there is *some* commercial aspect (the scammers' Achilles heel - is this the last mythology reference? Who knows!) in the scam in question, these should have at least some practical effectiveness.

In Court

Relief: When it comes to cases concerning brand misuse, the most common relief granted by Indian courts is injunctive - particularly at the interim stage. To deal with the hydra-nature of the digital violations, courts in India have of late started granting 'dynamic' injunctions as well.[8] Further, in cases where the scammers / infringers are found to be 'habitual offenders', courts may also grant damages - even exemplary damages[9].

At Domain Name Dispute Resolution Fora

The popular forums - World Intellectual Property Organization (WIPO) and National Internet Exchange of India (NIXI) - share a similar process when it comes to addressing issues relating to domain name scams. NIXI deals with the domain names with an .in ccTLD extension, while WIPO deals with gTLDs / select ccTLDs, etc. notified by it[10]. The three elements that need to be fulfilled for a case to be successful before WIPO / NIXI are i) brand owner's rights in the trademark in question; ii) the domain name in question being identical or confusingly similar to the trademarks; and iii) the scammers lack of any rights or legitimate interests in the domain name. When it comes to the third element specifically, WIPO and NIXI have independently held that domain names registered and run exclusively for scams and frauds inherently carry a bad faith element within them and the presumption of a lack of legitimate interest is evident.[11] Habitual offences are again a factor that is considered by NIXI and WIPO both.[12]

Limited Scope: WIPO and NIXI cannot adjudicate over cases where the domain name per se is not similar to the brands / trademarks in question - even if the website hosted thereon seeks to create an association. In the latter case, an action would lie only in a court of law.

Relief: The scope of 'relief' granted by WIPO / NIXI is limited to the transfer or cancellation of the domain name - transfer and maintenance is usually the preferred option for brand owners, so that the domain name remains in the control of the brand owner instead of being released in the public domain for (re)acquisition.

Takedown Requests and Buybacks

Internal grievance mechanisms of the domain name registrars or e-commerce platforms - as the case maybe - can often be used to get the domains, websites or 'store' pages taken down.

Criminal Actions

Although criminal enforcement is available in theory, there's a lot of nuances that go into deciding what sort of enforcement action to take and what grounds to claim, including questions of local jurisdiction, cause-of-action, jurisdiction where the scammers have their assets, etc. More importantly, in India, criminal enforcement actions often involve a lot of physical coordination and liaising with law enforcement agencies. Outside of these logistics, though - if the facts of a scam / fraud mandate it, there are several central and state agencies (including a cybercrimes division under the police department) that can be contacted in such matters, some of which may have overlapping functions.

Like we said before, the 'selection' of the correct remedy from the above (and others that might be available depending on the specifics of a case) is crucial and would depend on the facts of the case as well as the scale of misuse. At the end of the day, while enforcement here is not as straightforward as it is in more conventional brand misuse cases, there's more than enough to make the Icarus-es (Icarusi? Scammers.) realize they flew too close to the sun!

An Apple a Day.....Preventive Measures

Customer Awareness: The basis of all prevention rests on consumers being more and more aware of the general scams doing the rounds around the web, and also the specific nature of scams that could exploit and misuse a particular brand. A dedicated grievance / submission portal for the customers to submit their grievance (towards evidence collection) can also be considered, especially for online platforms.

Registration of Trademarks: Most of the 'legal recourses' mentioned above would either require, or just make the process a whole lot easier, if the brand owners have their major trademarks registered in India.

Monitoring / Policing: Periodic monitoring of the internet space would help the brand owners be more aware of whether their trademarks are being misused.

Footnotes

1. Ishi Khosla v. Anil Aggarwal and Anr. [2007 (34) PTC 370 Del], where it was held that in the internet age, it is possible for a unique enough business as well as related brands to become popular overnight.

2. Consuming public, per the widely accepted jurisprudence in India, is considered to be one possessing an 'average intelligence' and 'imperfect recollection'. In some cases, the distinct class, ability to discern and associate, paying capabilities and other similar out-of-the-ordinary characteristics of the consuming public could also be taken into consideration - but this is not the general rule of

4. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

5. Annexure 1 to the Cert-In Directions

6.https://rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=10477; https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=5111&Mode=0

7. Section 29(9) provides for trademarks infringement through *spoken* or written words.

8. See *Disney Enterprises, Inc. & Ors. versus Kimcartoon.to & Ors., CS(COMM) 275/2020*

9. See *Nippon Steel & Sumitomo Metal Corporation v. Kishor D Jain & Anr.*

10. https://www.wipo.int/amc/en/domains/gtld/

11. See *DXC Technology Company v. DXC Technology Company, Case No. INDRP/1292 (NIXI January 6, 2021)*

12. See *Dell Inc. v. Ram Selvam, Case No. 1333 (NIXI March 22, 2021); ASSA ABLOY A v. Yitao, C/o Apex Consulting, Case No. INDRP/1501 (NIXI, March 25, 2022)*

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

AUTHOR(S)

Manavi Jain
G&W Legal

Arjun Khurana
G&W Legal

Dishti Titus
G&W Legal