INDIA'S FIRST MAGAZINE ON LEGAL AND CORPORATE AFFAIRS

LEX WITNESS

Volume 12 Issue 10 | Aug-Sept 22 Anniversary Special Issue

₹ 100 US $10 UK £6

Anniversary Special

14th Year of Publishing

INDIA'S FIRST MAGAZINE ON LEGAL AND CORPORATE AFFAIRS

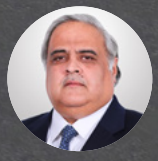
LEX WITNESS

Volume 12 Issue 10 | Aug-Sept 22 Anniversary Special Issue

₹ 100 US $10 UK £6

compliance cues

P70



Ameet Datta
Partner
Saikrishna & Associates

Suvarna Mandal
Partner
Saikrishna & Associates

ESG & more

P105

Alok Dhir
Founder & Managing Partner
Dhir & Dhir Associates

Poonam Bisht
Chief Executive Officer
Dhir & Dhir Associates

expert speak

P66

Guranpreet Singh Sarna
Partner
Dhir & Dhir Associates

Shikha Singh
Principal Associate
Dhir & Dhir Associates

P80

Tejveer Singh Bhatia
Partner
Singh & Singh Law Firm LLP

P87

Meghana Chandorkar
Partner
TMT Law Practice

P109

Jayanta Kar
Partner
S. Jalan & Co.

Soumik Chakraborty
Principal Associate
S. Jalan & Co.

P116

Ashu Kansal
Partner
Adhita Advisors

Rachit Mathur
Associate
Adhita Advisors

IN CONVERSATION WITH P62

Somesh Tiwari
Managing Partner
Vardharma Chambers

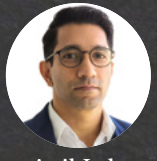
RENDEZVOUS P77

Partha Roy
Head - Legal & Contracts,
SPML Infra

TETE-A-TETE P84

Vani Mehta
General Counsel
GE South Asia

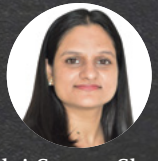
COUNSEL CORNER P92



Anil Lale
General Counsel
Viacom 18

IPR CORNER P97

Ananyaa Banerjee
Managing Associate
S.S. Rana & Co.



Shilpi Saurav Sharan
Senior Associate
S.S. Rana & Co.

LET'S ARBITRATE P107

S. Ravi Shankar
Sr. Partner
Law Senate

YOUR WITNESS PLEASE!

Rogue Websites Challenges, Initiatives & Way Forward

Tejveer Singh Bhatia

The COVID-19 pandemic dominated 2020- 2021. In these two years of COVID-19 the world has not only faced health issues, but the world has seen a downward trajectory of growth in economy owing to lockdowns imposed by the Government to break the chain of COVID-19. These lockdowns have seen various small industries/factories shutting their shops and thus, causing a large-scale unemployment. This unemployment has left us vulnerable to frauds in fanciful hope of a gainful employment.

During the same period of 2020-21, we have seen a huge growth in 'Work from Home' culture around us adopted by various National and Multi-National Companies. The Work from Home culture along with the unemployment caused due to COVID-19 has created an opportunity for Cybercriminals to exploit the vulnerabilities of the society as remote working has become a reality and a norm. We are all more exposed to cyber fraud due to the inevitable digital dependence, and this has resulted in cases of financial cybercrime being at an all-time high, with the numbers appearing to be on the rise.

CYBERCRIMINALS ARE ATTEMPTING TO EXPLOIT WELL KNOWN TRADEMARKS/TRADENAMES OF COMPANIES

Increased online activity due to the new normal of working remotely has led to a significant surge in Cybercrimes. There are various means and methods adopted by Cybercriminals to affect these frauds. One of such methods adopted by Cybercriminals is to purchase a domain name which comprises of a well-known trademark/tradename of a company which also contains keywords like 'Jobs', 'Recruitments', 'Franchise', 'Franchisee' 'Dealership' 'Distribution' 'Distributorship' etc.

These domain names are then used to host websites to lure the members of the public into believe in that the said websites/domain names are legitimate websites belonging to the said company and are offering jobs, distributorship, franchisee etc. through these websites. These websites are carefully created using the look and feel and the colour scheme which are similar to the company's original website. This is done so to create a sense of legitimacy to these fraudulent websites. These websites also use various marks and trademarks used by the company's original website. The addresses

SINGH & SINGH

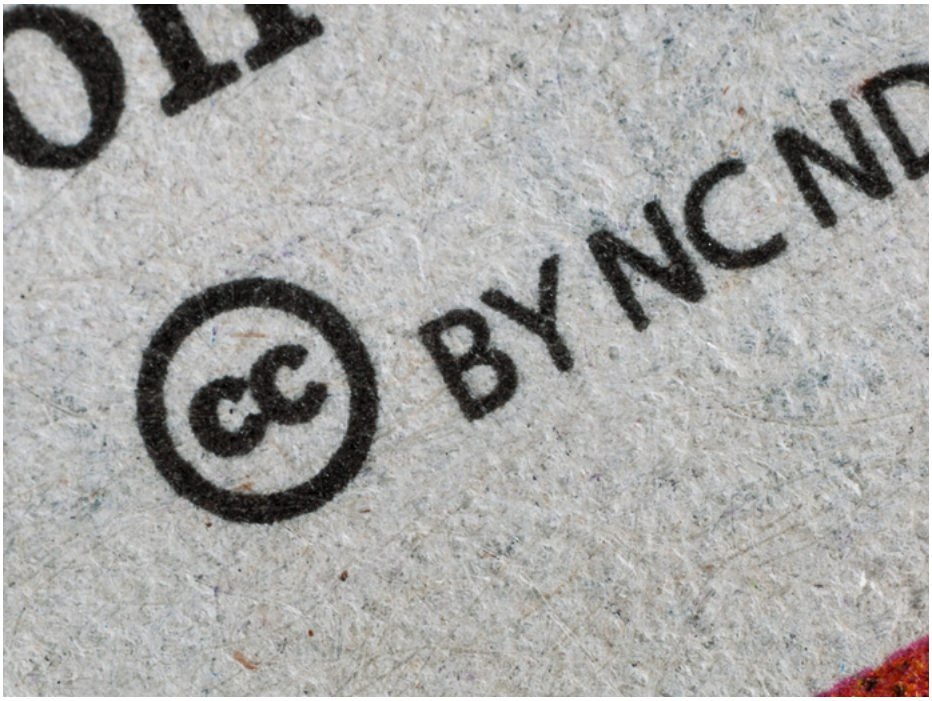
C-139, Defence Colony
New Delhi - 110024, India
T: +91 11 - 4982 6000 to 6099
E: email@singhandsingh.com

and the phone numbers given on these fraudulent websites are same as that of the company. However, the email address given in the website is fraudulent.

These fraudulent websites would generally provide for an inquiry form which a prospective victim would fill up providing his name, telephone number, email address etc. Upon filling these forms, the Cybercriminals then contact the prospective victims from different email IDs which would contain well-known trademark of a company to create an identity with the company. The Cybercriminals would provide a vendor registration form wherein the Cybercriminals ask for various details of the victim. These forms would also have the logo of the Company.

Once these forms are filled by the prospective victims, the Cybercriminals then seek a registration fee from the prospective victims. The registration fee is generally asked by way of a confirmation letter which would again use well-known trademark of the company also the bank account is in a similar name as that of a company. Once, the Cybercriminals receive the registration fee in their account, they have important personal financial information, such as telephone number, email ID, Account number, name of the bank, date of birth, etc., of the victims in their hands and the same could be exploited to extort money from the victims. However, in most cases, it is seen that most of the money is taken by the Cybercriminals as registration fee in the name of providing job, dealership, franchisee and thereafter, for providing goods and services.

In most of the cases, it is seen that the websites used for these frauds are



anonymous in nature and it is virtually impossible to locate the owners of such websites or to get contact details of such owner as the information provided in the public domain by Cybercriminals is either incomplete or incorrect. Most of the fraudulent websites hide behind domain privacy services offered by various organizations such as Domains by Proxy LLC/Private Registry Authority. As such, the Cybercriminals are able to hide behind a veil of secrecy and the contact details are not disclosed publicly to protect their so-called privacy.

This being the modus operandi of the Cybercriminals, these Cybercriminals further exploit advertisement services such as Google Ads Service to ensure that their name is displayed as the first link if someone searches for the well-known trademark of the company along with keywords such as 'Franchisee', 'Jobs', 'Distributorship' etc. As a result, innocent victims fall prey to these Cybercriminals and are losing their hard-earned money in these times when we all are recovering from the effects of COVID-19.

ACTIONS TAKEN BY THE OWNERS OF THE TRADEMARK AND DIRECTIONS OF THE COURT

Various companies in India have approached Courts in India having such problems. The Hon'ble Delhi High Court in recent past while dealing with similar issues, has passed interim orders directing the domain name Registrars to suspend/block/delete the domain names mentioned in the plaint. Further, in some of matters, Department of Telecommunication and MeitY have been asked to issue directions to all the ISP providers to block other websites which may be subsequently notified by the affected parties. The Registrars are also directed to provide details of the persons who have registered the offending

domains along with their complete contact details, postal address, email address, bank account and telephone numbers etc. The registrants of the offending domain names have been directed to pull down the websites and to cease using the domain names with immediate effect. Further, Google has been restrained from making available well-known trademarks as Ad words in their Google Ads Services.

Recently, the Hon'ble Delhi High Court taking note of 28 such matters and the difficulties in restraining the process of registration of infringing domain names due to large number of country code top level domains, generic top level domain, international country code top level domain and international generic country code top level domains with various extensions has passed a detailed order observing that in some of the cases a Special Investigation Team has been constituted by Cyber Cell, Delhi Police. However, the investigations are continuing. The Hon'ble High Court further took notice of various police reports wherein it was stated that in order to trace various bank accounts and payment gateway, cooperation of National Payment Corporation of India (NPCI) was required as it was extremely onerous to follow-up with each bank in each matter. Further, cooperation of Internet Service Providers and Telecom Service Providers was also requested by Delhi Police in the status report. The Hon'ble Delhi High Court in this view of the matter, directed a joint meeting of members of Delhi Police along with members of NPCI, DoT, MeitY and CERT-In to have a cohesive and coordinate strategy to deal with this menace of fraudulent websites. It was also recorded on behalf of MeitY that as on date there are no regulations to ensure that DNRs, not located in India, follow the orders of the Court or executive instructions. However, this matter is being discussed in the government and the recommendation/proposal for such regulations shall be placed before the Court on behalf of the Government.

ICANN also appeared before the Delhi High Court and made its submissions. The Delhi High Court recorded in detail various submissions of ICANN, inter alia, stating that ICANN Agreements do not oblige DNRs to extend privacy protection feature in case of blatant infringement and fraudulent activities. It was further submitted that all the registries and DNRs as per the Agreement, have to abide by and give effect to orders passed by Competent Courts, Government Authorities etc.

The Hon'ble Delhi High Court taking note of the submissions made by various parties present before it, further directed DoT and MeitY to give recommendations on the following aspects:

"(i) The manner in which the details of the domain name registrants, can be verified by the DNRs, at the time of registration of domain names;

(ii) The manner in which the privacy protect feature and proxy servers are made available: whether it is only upon a specific registrant choosing the said option, rather than as a standard feature as part of a 'bundle'.

(iii) If the owner of a well-known brand or a trademark contact any DNR, the manner in which the data related to the registrant can be provided, without the intervention of a Court, or any governmental agency;

(iv) Whether the identity of the owner of a domain name, which consists of a registered trademark or a known brand can be verified at the time of registration itself;

(v) If a specific link could be provided by the CGPTDM, covering a list of well-known marks, maintained by the Registrar of the Trademarks, or declared by any Court of law, which can then be used for expedited blocking of domain names consisting of such marks;

(vi) If there can be any agency that can be identified in India, such as NIXI, who can be made a repository of the data concerning the registrant, or an agency through which the data could be transmitted by the DNR, upon verification by NIXI, in case a trademark owner has a grievance against a specific domain name;

(vii) If any directions are issued to the DNRs, and the same are not implemented, the manner in which the implementation of the said orders can be ensured;

(viii) Since almost all domain names are registered only after payments are made through credit card, or other online payment methods or apps, is it possible, upon request by any identified agency, to provide the information relating to the person who has made the payment, to the trademark owners. This should be discussed in the aforementioned meeting to be held on 30th August 2022."

CONCLUSION

It is always seen that these Cybercriminals have always been a step ahead of law. The initiative taken by the Hon'ble Delhi High Court to club all the matters and to hear them together to have a comprehensive framework to deal with such Cybercrimes is a welcome step and would provide the industry the much-needed confidence that their marks will be well protected in the ever expanding digital world. However, the steps taken by the Hon'ble Delhi High Court once again expose how far is the extant regulatory framework from the realities of the Cyberspace. It also highlights the fact that while the Regulator should be having a foresight to visualize the problems of growing cyberinteractions and possibility of multi-level frauds in metaverse, we are still struggling with the age-old issues of cybersquatting and fraudulent websites. We hope that the present initiative of the Hon'ble Delhi High Court acts as a wake-up call for the Regulators and the issues before the Hon'ble High Court find the meaning resolution both in judicial orders and regulations by the concerned Regulators.

[1]*Order dated 06.07.2022 in CS (Comm) No. 447/2022 – Havells India Ltd. Vs. Ashok Kumar/John Doe & Ors.*
[2]*Order dated 03.08.2022 in CS (Comm) No. 135/2022 – Dabur India Limited Vs. Ashok Kumar & Ors. along with other connected matters.*

Tejveer Singh Bhatia is currently working as a Partner at Singh & Singh Law Firm LLP. He has been practicing in the field of Telecom & Broadcasting laws since then. He has vast experience of being involved litigations regarding various spectrum of law including IPR. He holds expertise in laws relating to Content Regulation and other Regulatory aspects regarding Broadcasting & Telecom Sectors. He regularly conducts Civil and Criminal raids vis-à-vis Anti-Counterfeiting including Custom Recordals and has vast experience in relation to Arbitration & Constitutional Law.