science editing
pISSN 2288-8063
eISSN 2288-7474
Sci Ed 2018;5(1):49-52
https://doi.org/10.6087/kcse.118

Case Study

Arbitral action and preventive methods against predatory journal practice

Sung Pil Park[1], Eric Yong Joong Lee[2,3], Ji Hee Suh[3]

[1]Master of Intellectual Property Program, Korea Advanced Institute of Science and Technology, Seoul; [2]College of Law, Dongguk University, Seoul; [3]YIJUN Institute of International Law, Seoul, Korea

Abstract

As open access model of journal publication increases, predatory journals, which deceive scholars to publish journals in fake database websites and exploit them for publishing fee, is also increasing. There are two types of predatory journals. First, journal hijacking and cybersquatting generally create fake database website by mimicking authentic database website, thereby defrauding scholars for publication fee. Second, journal phishing use scam emails to steal scholars' personal information. If scholars suffered damage from predatory journals, scholars can take either arbitral or judicial actions. Arbitral action follows arbitrational resolution process termed Uniform Domain-Name Dispute-Resolution Policy. Scholars can join Uniform Domain-Name Dispute-Resolution Policy proceeding with legal entity that has right to authentic database website, which will result in cancellation or transfer of fake database website. In contrast, scholars can take judicial action under Anticybersquatting Consumer Protection Act, which may help scholars to recover an actual monetary damage from predatory journals. Nonetheless, taking precaution to avoid predatory journals is the best course of action, rather than going through arduous cure procedures. Scholars may prevent predatory journals by carefully examining fake database website names or email addresses, or observing unreasonable number of published article issues in predatory journal websites.

Keywords

Asian Domain Name Dispute Resolution Center; Cybersquatting; Journal hijacking; Journal phishing; Uniform Domain-Name Dispute-Resolution Policy

Received: January 14, 2018
Accepted: February 12, 2018

Correspondence to Ji Hee Suh
suh23@wisc.edu

ORCID
Sung Pil Park
http://orcid.org/0000-0002-7778-4814
Eric Yong Joong Lee
http://orcid.org/0000-0001-5640-490X
Ji Hee Suh
http://orcid.org/0000-0003-3761-9838

Introduction

In June 2016, a scholar in Korea submitted his manuscript to phishing email 'jeet@jeet.us' by following the instructions on the phishing website (http://www.jeet.us), because he misunderstood the phishing website as the authentic journal database website, *Journal of Electrical Engineering and Technology* (JEET) [1]. He soon received a confirmation reply email of acceptance

and expected date of publication. However, there was no further progress. He consequently inquired about his publication at 'jeet@kiee.or.kr,' official email of JEET. During the correspondence, the scholar found out that the previous email address, jeet@jeet.us, which he sent his manuscript at, was a phishing email. Because there was no monetary loss due to absence of request for publication fee, police investigation was unavailable. This is a typical case of predatory journal practice, which can be referred to as journal phishing, journal hijacking or cybersquatting. Predatory journal practice shows new legal challenge to contemporary academic journal publications. This article will touch on arbitral actions and prevention methods.

Alternative Dispute Resolution

In 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) was formed in order to assume responsibility for administering domain name systems internationally [2-4]. ICANN's intellectual property policy then soon established a compulsory arbitral resolution process called the Uniform Domain-Name Dispute-Resolution Policy (UDRP), for dealing with cases of cybersquatting [2,4]. By imposing contract between an accredited domain name registrar and its customer (domain name registrant), UDRP makes every registrant to adhere to register warrant terms [3]. The register warrant terms include, but not limited to: (1) to the best of the registrant's knowledge, the registration of the domain name will not infringe or violate the rights of any party; (2) the domain name is not being registered for an unlawful purpose; (3) the domain name will not be knowingly used in violation of any applicable laws or regulations [5].

Any individual or legal entity that owns trademark can initiate the UDRP proceeding by filing a written complaint to an approved "dispute resolution service providers" against registrant who violated warrant terms [2,3]. The approved dispute resolution providers exist internationally, including the World Intellectual Property Organization mediation and arbitration center and the Asian Domain Name Dispute Resolution Center (ADNDRC) [2,3]. The ADNDRC Seoul office manages disputes in Korea [6].

Even though individual scholars do not own journal database or domains' trademark, they may potentially join journal database owners or administrators in the UDRP proceeding. There are two grounds that support this potential class proceeding. Foremost, the UDRP proceeding allows multiple parties to file a single complaint where the parties have a common interest in the trademark allegedly infringe [5]. Hence, the UDRP proceeding may allow scholars who are harmed by journal hijacking to join the complainant, because the hijacked website potentially infringed scholars' right and trademark in the journal.

In addition, scholars' potential monetary or security damage from journal hijacking will satisfy the UDRP proceeding's substantive requirements for a successful complaint. There are three substantive requirements for the UDRP proceeding's successful complaint [3,5].

First, the domain name should be identical, or confusingly similar to a trademark or service mark in which the complainant has rights [5]. The UDRP proceedings often held that domain names comprised of misspellings of marks, to the extent that they are identifiable as misspellings, to be confusingly similar to authentic trademarks [5]. Because cybersquatters generally utilize typosquatting to create confusingly similar domain names to that of authentic journal database, the first requirement can be easily satisfied.

Second, the Respondent should not have right or legitimate interest in the domain name [3,5]. If cybersquatters purposely hijack journals by mimicking authentic journal database domains, they certainly do not have right or legitimate interest in the authentic domain name. Hence, the second requirement can be also satisfied.

Third, the domain name should be registered and used in bad faith [5]. In *Caesar World, Inc. v. Stephens*, the UDRP proceeding panel held that the use of domain name to attract internet users for commercial gain, by creating confusingly similar domain name or endorsing complainant's mark, is an example of bad faith [7]. In fact, the UDRP panel penalizes almost all manner of cybersquatting, because cybersquatting satisfies UDRP proceeding's substantive requirements for a complaint in relatively straightforward manner [8].

Consequently, if a scholar who lost monetary or security interest joins the UDRP proceeding, his/her damage may be used to satisfy the bad faith requirement [8]. In this case, the UDRP proceeding may allow the scholar to join the complainant by holding that the scholar's interest is at the stake of the proceeding.

Arbitral Procedure in Korea

In Korea, there are two different alternative dispute resolution centers against cybersquatting. The first center is the Internet Address Dispute Resolution Committee (IDRC). IDRC was established in 2004 in order to administer national domain name ending with '.kr' [9]. The second center, ADNDRC Seoul office, regulates disputes arising out of general domain names that are registered in ICANN [6]. ADNDRC Seoul office thus assumes the World Intellectual Property Organization's position in Korea [9].

If a Korean scholar suffers from journal phishing or hijack-

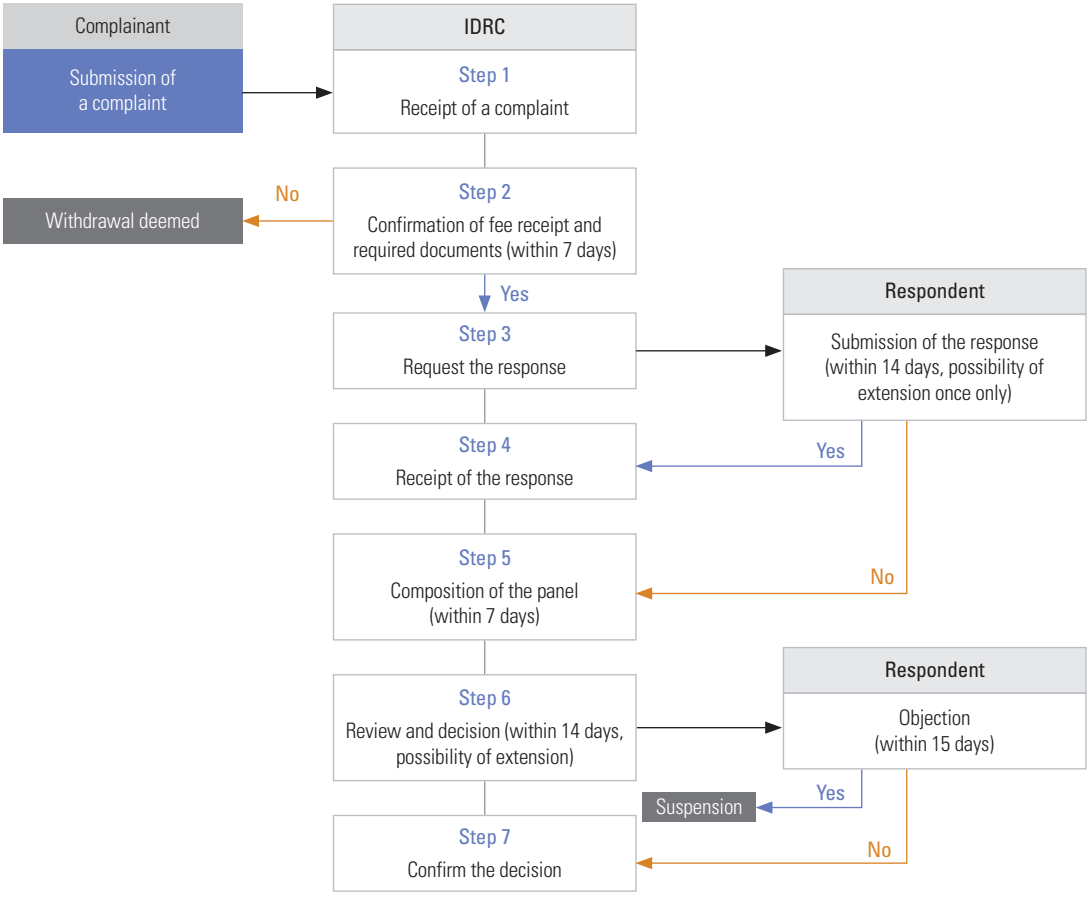

Fig. 1. Arbitral proceeding steps in Korea under the Internet Address Dispute Resolution Committee (IDRC) guidance.

ing mimicking national domain (.kr) database, s/he can commence arbitral proceeding by going through seven steps under the IDRC guidance (Fig. 1) [10]. First, scholar should prepare complaint and submit it to the IDRC. IDRC will then send receipt to the scholar [10]. Second, IDRC will collect process fee and documents including complaint. Then, it will request limitation on domain name change to domain registrar and registrant [10]. Third, IDRC will request response brief from the registrant [10]. The registrant has 14 days to respond from the day the registrant receives the IDRC request for response brief [10]. Fourth, IDRC will collect response brief from the registrant [10]. Even if the registrant does not submit the response brief, the UDRP proceeding will continue [10]. Fifth, IDRC will appoint arbitral panel with either one or three personnel. Sixth, arbitral panel will issue the decision generally within 14 days of the appointment of the panel [10]. Lastly, if the complainant prevails and the registrant does not appeal within 15 days, the domain name registrant will either cancel the domain name registration or transfer the domain to the complainant [10].

The UDRP proceeding in Korea is similar to the IDRC arbitral proceeding, except for the following few steps [11]. First, scholar can submit the complaint to 'kidrc@adndrc.org' or using online submission system [11]. Second, the registrant has 20 days, instead of 14 days, to respond to the complaint [11]. Third, ADNDRC Seoul office appoints either one or three personnel arbitral panel instead of IDRC [11]. Finally, if the complainant prevails, the registrant has 10 days to appeal in the court [11].

Because the UDRP proceeding's remedies are limited to the cancellation of the domain name registration or transfer to the complainant, scholar's potential monetary damage will not be compensated [5]. Consequently, scholar can initiate legal proceedings either before or after, or even at the parallel track with the arbitral proceeding. It is important to note that arbitral decision is not binding on courts and the judicial decision overrides arbitral decision [5].

Prevention

Here are few guidelines that scholars and journal database administrators can follow in order to avoid cybersquatting. First, carefully examining spelling or symbols of hijacked journal's domain name may help scholars to discern authentic and fraudulent domain names. Second, observing suspicious journal website's unreasonable number of published article issues and index may help scholars to avoid journal hijacking. Third, carefully observing spear phishing email's "from" and "reply to" sections may prevent journal phishing. In spear phishing email, address of "from" section is generally different from "reply to" section. In addition, scholars should avoid any embedded links or downloading suspicious attachment files. Fourth, ignoring prize or warning messages about account closing will prevent journal phishing. It is best to ignore and avoid these click baits.

Conclusion

In order to prevent journal phishing and hijacking, scholars and academic community must increase awareness and heighten knowledge of possible preventive and protective methods. Recently, academic journals' editors are constantly threatened by possible cyber-attacks, which seriously damage the academic integrity of scholars and institutions.

Even though arbitral and legal resolutions exist to counteract cybersquatting, as with all other internet frauds, efforts to cure the damage may be limited in practice. Therefore, academic institutions and scholars should be always attentive to preventive measurements against possible journal phishing and hijacking attacks.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgments

This work was supported by the research program at Dongguk University, Seoul, Korea.

References

1. Choi J. Impersonation of Journal of Electrical Engineering & Technology journal website. Sci Ed 2017;4:76-9. https://doi.org/10.6087/kcse.99
2. Merges R, Menell P, Lemley M. Intellectual property. In: The new technological age. 3rd ed. New York, NY: Aspen Publishers; 2003. p. 647-59.
3. Jehoram T, Nispen C, Huydecoper T. European trademark law: community trademark law and harmonized national trademark law. Alphen aan den Rijn: Kluwer Law International; 2010.
4. Goldstien P, Reese A. Copyright, patent, trademark and related state doctrines: cases and materials on the law of intellectual property. 6th ed. New York, NY: Foundation Press; 2010.
5. Heavner B, Lemper T. Remedies for trademark infringement and unfair competition on the internet. In: Banner B, editor. Trademark infringement remedies. Washington, DC: BNA Books; 2007. p. 4-13.
6. Internet Address Dispute Resolution Committee. ADNDRC Seoul office [Internet]. Naju: Korea Internet & Security Agency [cited 2018 Jan 9]. Available from: https://www.idrc.or.kr/rc/dmNomal/adndrcSeoul.jsp
7. WIPO Arbitration and Mediation Center. Administrative panel decision: Caesars World, Inc. v. Stephens, D2001-0553 [Internet]. Geneva: World Intellectual Property Organization; 2001 [cited 2018 Jan 20]. Available from: http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0553.html
8. McManis C. Intellectual property and unfair competition in a nutshell. St. Paul, MN: West Academic Publishing; 2009.
9. Internet Address Dispute Resolution Committee. Foundation purpose and history [Internet]. Naju: Korea Internet & Security Agency [cited 2018 Jan 9]. Available from: https://www.idrc.or.kr/rc/intro/introPurpose.jsp
10. Internet Address Dispute Resolution Committee. IDRC procedure [Internet]. Naju: Korea Internet & Security Agency [cited 2018 Jan 9]. Available from: https://www.idrc.or.kr/rc/dm/dmProcedure.jsp
11. Internet Address Dispute Resolution Committee. ADNDRC Proceeding [Internet]. Naju: Korea Internet & Security Agency [cited 2018 Jan 7]. Available from: https://www.idrc.or.kr/rc/dmNomal/dmNomalProcedure.jsp