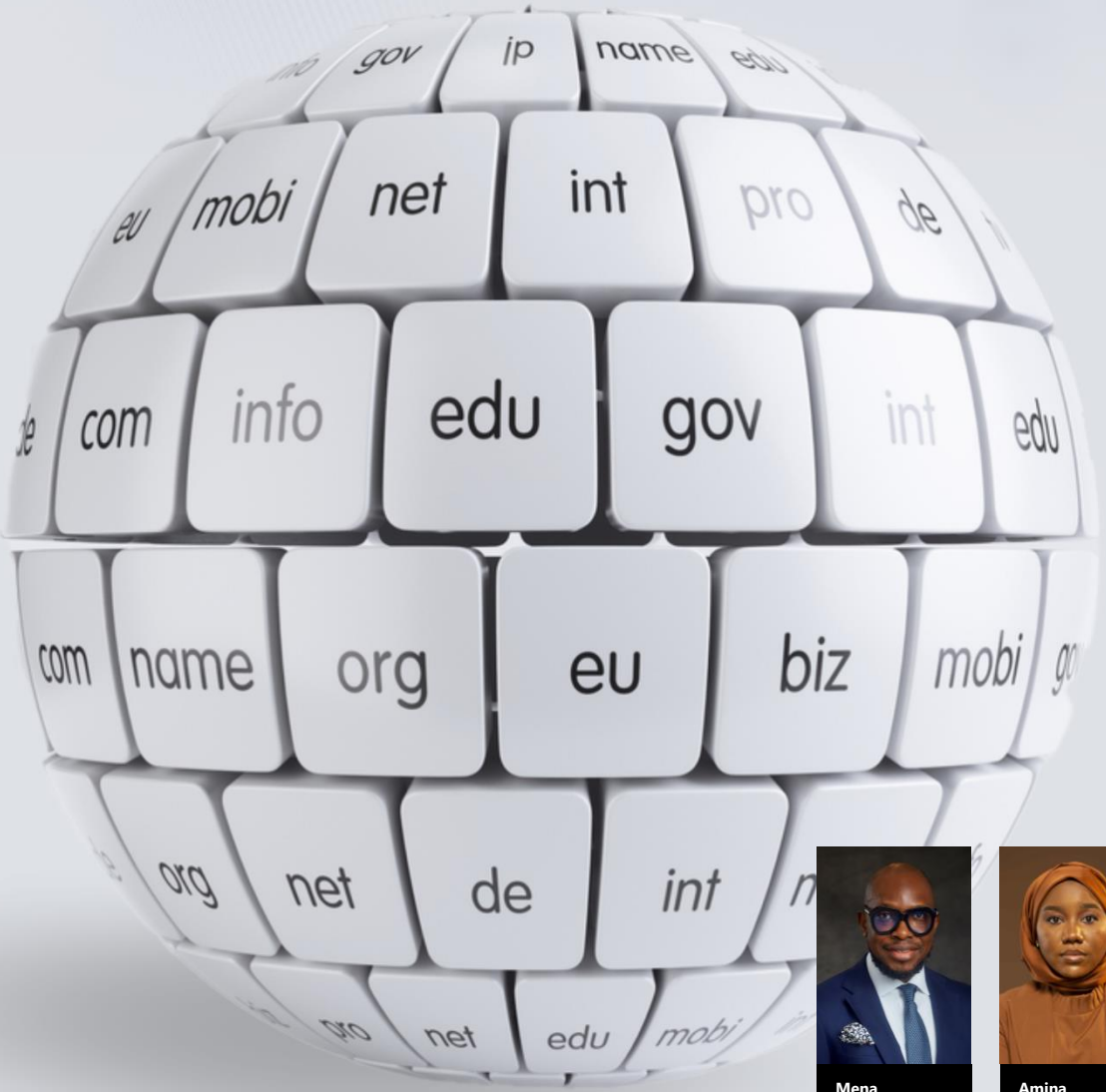
UDO UDOMA & BELO-OSAGIE

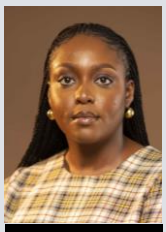
DID YOU KNOW SERIES
(Vol. 4)

CYBERSQUATTING IN NIGERIA: CHALLENGES AND COUNTERMEASURES



Mena Ajakpovi
Partner

Amina Ibrahim
Partner


Emiloluwa Imolehin
Associate


Victoria Sunday
Associate

Introduction to Cybersquatting

In our digitally driven world, where the internet is a cornerstone of commerce, communication, and information dissemination, cybersquatting has emerged as a serious threat. The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 in Nigeria addresses this menace, specifically in Section 25, which defines and penalises cybersquatting.

Cybersquatting is the bad-faith acquisition and use of domain names similar or identical to existing trademarks, aiming to profit from, mislead, destroy reputations, or prevent rightful ownership. This newsletter explores the legal definition, challenges, and countermeasures related to cybersquatting in Nigeria.

Current Landscape of Cybersquatting in Nigeria

Cybersquatting has grown alongside the rise of internet usage in Nigeria, affecting businesses and individuals alike. Victims face financial losses, reputational damage, and legal battles as cybersquatters exploit domain names for malicious purposes.

Legal Framework for Combating Cybersquatting in Nigeria

The Cybercrimes Act

The Cybercrimes Act[1] criminalises cybersquatting. Victims can report suspicious activities to law enforcement, leading to prosecution. Convicted individuals face up to two years in prison and/or a fine of up to N5,000,000 (five million Naira).

Uniform Domain Name Dispute Resolution Policy (UDRP)[2]

The Uniform Domain Name Dispute Resolution Policy (UDRP), developed by ICANN and WIPO, provides a mechanism for resolving domain name disputes. To succeed, a complainant must prove:

- The domain name is identical or confusingly similar to their trademark.
- The registrant has no legitimate rights to the domain name.
- The domain name was registered and is used in bad faith.

[1] S. 25, Cyber Crimes (Prohibition and Prevention, Etc) Act, 2015
[2] https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en

Overview of the UDRP Administrative Procedure[3].

1. Submission of a Complaint to an ICANN-accredited dispute resolution service provider selected by the Complainant, such as the WIPO Center ("the Center");

    i. The complaint must be filed electronically, and a copy of the complaint must be sent to the Registrars and Respondent.[4]
    ii. The Center acknowledges receipt and then requests specific details concerning the disputed domain name.
    iii. The Center then conducts compliance formalities and notifies the Complainant and the Respondent of any deficiencies in the application. Applications not remedied within 5 days of the notification are deemed withdrawn.
    iv. Where there are no deficiencies with the application, the Center formally notifies the Respondent in line with the Rules. This forms the formal commencement of the proceeding.

2. Submission of a Response by the individual or entity against whom the Complaint is directed.

    i. The response must be filed within 20 working days.

3. Appointment by the chosen dispute resolution service provider of an Administrative Panel consisting of one or three individuals who will adjudicate the dispute.

4. Issuance of the Administrative Panel's decision and notification to all relevant parties.

    i. The Panel is required to forward their decision to the Center within 14 working days from the date of their appointment.

    ii. The Center must then notify ICANN within 3 working days from the date of receipt.

[3] https://www.wipo.int/amc/en/domains/guide/#a
[4] Para 3(b) UDRP Rules

5. Implementation of the Administrative Panel's decision by the concerned registrar(s) if the decision entails the cancellation or transfer of the domain name(s) in question.

Nigeria Internet Registration Association (NiRA)[5]

NiRA oversees the .ng domain names and offers a dispute resolution process for cybersquatting cases. Complaints can lead to the transfer or cancellation of disputed domain names if they meet the criteria of being identical or confusingly similar to existing trademarks, registered in bad faith, or lacking legitimate interest by the registrant.

One notable case of Cybersquatting in Nigeria is **Konga Online Shopping Limited v. Rocket Internet GmbH[6]** where Konga Online Shopping Limited ("Konga") filed a complaint with the WIPO Arbitration and Mediation Centre against Rocket Internet GmbH and Arnt Jeschke over the domain name <konga.sc>.

Konga claimed the domain name was identical to its trademark and registered in bad faith. It alleged the domain was used as leverage for a declined partnership, intended to hinder Konga's expansion and support the "Jumia" franchise, and highlighted the potential for confusion due to prior use and common law rights to "Konga."

Rocket argued that <konga.sc> was a Seychelles country code domain and was irrelevant to Nigeria, and Konga had no trademark rights in Seychelles. It further claimed that the domain was intended for an online dating site, unrelated to Konga's business, asserted "Jumia" operations were distinct and Konga's focus was limited to Nigerian consumers and emphasised the domain registration predated Konga's trademark applications and launch of <konga.com>.

The complaint was dismissed as Konga failed to prove the domain was identical or confusingly similar to a trademark in which it had rights, per UDRP Rule 4(a).

Challenges Faced by Victims of Cybersquatting

Victims encounter significant financial losses, including legal fees and lost customers, including loss of reputation, as fraudulent websites misuse brands, erode consumer trust, and divert traffic away from legitimate sites.

Best Practices for Preventing Cybersquatting

1. **Register Business Names Early**: Secure domain names as soon as possible.
2. **Monitor Domain Names**: Regularly check for similar or identical domain registrations.

[5] https://nira.org.ng/domain-name-dispute-what-to-do/
[6] https://www.wipo.int/amc/en/domains/decisions/text/2014/dsc2014-0001.html

3. **Purchase Variations of Your Website Address**: Prevent cybersquatters from exploiting variations.
4. **Secure Domains and Trademarks**: Legal protection through trademarks and domain registrations.
5. **Regular Monitoring and Enforcement**: Stay vigilant and enforce your rights.
6. **Educate Employees and Customers**: Raise awareness about cybersquatting threats.

Global Perspectives on Cybersquatting

Countries worldwide face similar challenges with cybersquatting. International cooperation and shared best practices can help combat these threats. The UDRP offers a global framework for efficiently addressing domain disputes.

Conclusion

Cybersquatting is a persistent challenge in Nigeria. While the legal framework provides some protection, continuous efforts are needed to stay ahead of cybercriminals' evolving tactics. Nigeria can create a more secure digital environment and contribute to global efforts against cybersquatting by engaging in collaboration, awareness, and advanced technologies to empower businesses and individuals to protect their online assets and maintain digital integrity.

This update is for general information purposes only and does not constitute legal advice. If you need any legal advice in relation to your intellectual property assets or information about our practice offerings, please contact us at IPTeam@uubo.org.