

Trade Marks:

Unlocking Brand Protection *Part 6*

A Guide To Domain Name Protection In Nigeria



LAGOS | ABUJA | CALABAR

INTRODUCTION

In today's digital economy, a company's online presence is often as valuable as its physical presence. Unfortunately, it has become increasingly common for businesses and consumers to encounter fraudulent websites, cloned webpages, and misleading domain names designed to impersonate legitimate brands. In many cases, unsuspecting customers disclose sensitive information or make payments to cybercriminals, causing financial losses and reputational damage to the affected businesses.

A domain name is a critical component of a company's online identity. It serves as the address through which customers, partners, and stakeholders access a business online. As domain names become increasingly valuable commercial assets, businesses must take proactive steps to protect them from cybersquatting, impersonation, trademark infringement, and other forms of online abuse.

This article provides an overview of domain name protection in Nigeria, including registration and renewal strategies, dispute resolution mechanisms under the Nigeria Internet Registration Association (NiRA), the joint role of the World Intellectual Property Organisation (WIPO) and the Internet Corporation for Assigned Names and Numbers (ICANN), and the use of trademark infringement and passing off actions to recover or disable infringing domain names.

Why Domain Name Protection Matters

A domain name is more than just an internet address; it is often synonymous with a company's brand and goodwill. Effective domain name protection is important for several reasons:

1. **Brand Identity:** A domain name is frequently the digital embodiment of a business's brand. Losing control of a domain name or allowing third parties to register confusingly similar domains can undermine brand recognition and dilute the value of a company's intellectual property.
2. **Customer Trust:** Customers expect to interact with genuine websites. Fraudulent or deceptive domain names can mislead consumers, facilitate phishing attacks, and damage customer confidence in a business.
3. **Business Continuity:** A business that loses access to its primary domain name may experience disruptions in communications, e-commerce operations, and customer engagement. Effective protection measures help ensure uninterrupted online operations.
4. **Cybersecurity and Fraud Prevention:** Cybersquatters and malicious actors often register domain names that imitate legitimate brands to facilitate scams, phishing schemes, and other fraudulent activities. Domain name protection forms part of a broader cybersecurity and risk management strategy.

Domain Name Registration in Nigeria

To protect a domain name in Nigeria, businesses should take the following steps:

1. Choose an Accredited Registrar

Select a reputable domain name registrar accredited by the Nigeria Internet Registration Association (NiRA), the registry responsible for administering the .ng country code top-level domain (ccTLD).

2. Conduct Availability Searches

Before registration, verify that the desired domain name is available and does not infringe existing trademarks or business names. Searches should be conducted through the NiRA *WHOIS* database and relevant trademark registries.

3. Register Your Domain Name

Provide accurate ownership and contact information during registration. Businesses should ensure that domain names are registered in the company's name rather than in an individual employee's or contractor's name.

4. Align Domain Names with Trademarks

Where possible, businesses should register domain names that correspond with their registered trademarks. Trademark ownership can significantly strengthen a business's position in domain name disputes.

Domain Name Renewal and Maintenance

Securing a domain name is only the first step in protecting an online presence. Businesses must actively maintain their domain name registrations by ensuring that renewal mechanisms are in place, closely monitoring renewal dates, keeping registrant and contact information up to date, retaining administrative control over domain management accounts, and conducting periodic audits of their domain name portfolios.

Failure to renew a domain name may result in its expiration and subsequent registration by third parties.

DOMAIN NAME DISPUTE RESOLUTION IN NIGERIA: NIRA DISPUTE RESOLUTION POLICY (NDRP)

Nigeria has established a domain name dispute resolution framework through the NiRA Dispute Resolution Policy (NDRP)¹, which applies to *.ng* domain names.

Under the NDRP, a complainant may seek the transfer or cancellation of a domain name.² where:

- The disputed domain name is identical or confusingly similar to a name, trademark, service mark, or other identifier in which the complainant has rights;
- The registrant has no legitimate interest in the domain name; and
- The domain name was registered or is being used in bad faith.

Examples of bad faith include registering a domain name primarily for resale to the trademark owner, disrupting a competitor's business, or misleading consumers by creating confusion with an established brand.

Complaint Procedure³A complainant may file a complaint with an approved dispute resolution provider by submitting evidence of:

- Trademark rights or other proprietary interests;

¹ https://nira.org.ng/pdf/NIRA_DISPUTE_RESOLUTION_POLICY.pdf

² 6.1 of the NiRA Dispute Resolution Policy (NDRP). See also Paragraph 3 of Schedule A of the NDRP.

³ See Paragraph 4 of the NDRP

- Similarity between the trademark and the disputed domain name;
- Lack of legitimate rights by the registrant; and
- Evidence of bad faith registration or use.

Arbitration and Mediation: The NDRP provides a streamlined alternative to litigation through arbitration and administrative proceedings. Successful complainants may obtain the transfer or cancellation of the disputed domain name without resorting to lengthy court proceedings.

INTERNATIONAL PROTECTION FOR DOMAIN NAMES: WIPO ADMINISTRATIVE PROCEEDINGS FOR DOMAIN NAME DISPUTES

The World Intellectual Property Organisation (WIPO) is one of the leading dispute resolution providers authorised by the Internet Corporation for Assigned Names and Numbers (ICANN) to administer domain name disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP).

Where a trademark owner believes that a domain name has been registered and used in bad faith, the owner may file a complaint before a WIPO Administrative Panel. The proceedings are conducted entirely online and are generally faster and more cost-effective than traditional court litigation.

A WIPO Administrative Panel will typically consider whether:

1. The disputed domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
2. The registrant has no rights or legitimate interests in the domain name; and
3. The domain name was registered and is being used in bad faith.

Where these elements are established, the panel may order the transfer or cancellation of the domain name. Although WIPO panels do not award monetary damages, they provide an efficient mechanism for recovering domain names from cybersquatters and bad-faith registrants.

Several notable disputes illustrate the importance of WIPO proceedings. In *Shell International Petroleum Co. v. Allen Jones*⁴, the respondent registered the domain name *shell-nigeria.com* and replicated the appearance and content of Shell's legitimate Nigerian website. The panel found that the domain name had been registered and used in bad faith to mislead internet users and ordered that the domain name be transferred or removed.

Conversely, in *Konga Online Shopping Limited v. Rocket Internet GmbH*⁵, Konga sought to recover domain names containing the "Konga" brand. The complaint was unsuccessful because Konga was unable to establish sufficient trademark or common law rights in the relevant jurisdiction. The decision

⁴ *Shell International Petroleum Company Ltd. v. Allen Jones*. Case No. D2003-0821. <https://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0821.html>

⁵ *Konga Online Shopping Limited v. Rocket Internet GmbH, Arnt Jeschke*. Case No. DSC2014-0001. <https://www.wipo.int/amc/en/domains/decisions/text/2014/dsc2014-0001.html>. See also the recent case *Julius Blum GmbH v. Moshood Olatunji, Sunminers Nigeria Limited*. Case No. D2024-0199. <https://www.wipo.int/amc/en/domains/decisions/pdf/2024/d2024-0199.pdf> Where the panel ordered that the disputed domain name <blumnigeria.com> be transferred to the Complainant. See also, *TIME USA, LLC v. Chidipeters Okorie, TIME AFRICA MAGAZINE*. Case No. D2026-0880. <https://www.wipo.int/amc/en/domains/decisions/pdf/2026/d2026-0880.pdf> The panel also ordered that the disputed domain name <timeafricamagazine.com> be transferred to the Complainant.

highlights the importance of securing trademark registrations and maintaining evidence of goodwill before initiating domain name recovery proceedings.

For businesses operating internationally, WIPO administrative proceedings remain one of the most effective tools for enforcing trademark rights against cybersquatting, impersonation, and abusive domain name registrations.

TRADE MARK INFRINGEMENT ACTIONS AND DOMAIN NAMES

Domain names that incorporate or imitate registered trademarks may constitute trademark infringement where they create confusion regarding the source, sponsorship, affiliation, or endorsement of goods and services.

Under the Nigerian Trade Marks Act, trade mark owners may institute infringement proceedings against parties who use their registered marks without authorisation, including through domain names and websites.⁶

Courts may grant various remedies, including:

- Injunctions restraining the continued use of the infringing domain name;
- Orders directing the transfer of the domain name to the trademark owner;
- Damages or an account of profits;
- Delivery up or destruction of infringing materials; and
- Ancillary orders requiring internet intermediaries or registrars to disable access to the offending domain.

A favourable trademark infringement judgment may therefore serve as a basis for obtaining the transfer, suspension, or takedown of an infringing domain name.

CYBERSQUATTING UNDER THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT

Nigerian law criminalises cybersquatting under the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (as amended). The Act defines cybersquatting as the bad-faith registration or acquisition of a domain name to profit, mislead, damage another person's reputation, or prevent them from registering the name, where the domain name is:

- Identical or confusingly similar to a registered trademark;
- Identical or similar to another person's name; and
- Acquired without any lawful right or legitimate intellectual property interest.⁷

To establish cybersquatting, it must generally be shown that:

- a. The domain name was acquired in bad faith;
- b. The registrant intended to profit, mislead, damage a reputation, or block another person from registering the name;

⁶ Section 5 Of the Trade Marks Act

⁷ See Section 25 Of the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (as amended).

- c. The domain name is identical or confusingly similar to a registered trademark or another person's name; and
- d. The registrant has no legitimate rights or interests in the domain name.

Unlike the NDRP and UDRP, which mainly provide for the transfer or cancellation of domain names, the Cybercrimes Act impose criminal liability on cybersquatters.⁸ Victims may therefore pursue administrative, civil, and criminal remedies depending on the circumstances of the case.

PASSING OFF ACTIONS AND DOMAIN NAME PROTECTION

Even where a business has not registered its trademark, it may still be able to protect its brand through the common law tort of passing off. Passing off occurs where a person misrepresents its goods, services, or business as being associated with another business, thereby causing damage to the goodwill of that business. In the context of domain names, passing off may arise where a third party registers and uses a domain name that falsely suggests an association with an established brand, company, or service provider.

To succeed in a passing-off action, a claimant generally must establish:

- i. Goodwill or reputation in the relevant name, mark, or brand;
- ii. A misrepresentation by the defendant likely to deceive the public; and
- iii. Damage or a likelihood of damage resulting from the misrepresentation.

Where passing off is established, courts may grant injunctions and other relief that can be used to disable, transfer, or otherwise prevent the continued use of the offending domain name. Passing off is particularly valuable for startups, businesses with unregistered marks, and entities that have developed substantial goodwill but have not yet secured trademark registrations.

USING COURT ORDERS AND JUDGMENTS TO TAKEDOWN INFRINGING DOMAIN NAMES

In addition to administrative procedures such as the NDRP and UDRP, businesses may obtain court orders requiring the removal, suspension, transfer, or disabling of infringing domain names.

Depending on the circumstances, court orders may be directed to Domain registrars, Domain registries, Website hosting providers, Internet service providers, Search engines, or other intermediaries facilitating the infringing activity.

Such orders may arise from trademark infringement proceedings, passing off claims, anti-counterfeiting actions, consumer protection claims, or fraud-related litigation. Where a domain name is being used to facilitate phishing, impersonation, or other unlawful conduct, courts may also grant urgent interim relief to prevent ongoing harm pending the determination of the substantive dispute.

CONCLUSION

Domain names have become indispensable business assets and a critical part of brand protection strategies. Businesses operating in Nigeria should not only secure and maintain their domain names but should also understand the various enforcement mechanisms available when disputes arise.

⁸ Ibid

Whether through the NiRA's NDRP for .ng domains, ICANN's UDRP for international domains, trademark infringement actions, passing off claims, or court-ordered takedowns, businesses have multiple legal avenues for protecting their online identity. A proactive domain name protection strategy can help preserve brand value, maintain customer trust, prevent fraud, and ensure the continued integrity of a company's online presence.

CONTACTS



ROTIMI AKAPO

rotimi.akapo@advocaat-law.com



ADEYEMI OWOADE

adeyemi.owode@advocaat-law.com



INIMFON EKPENYONG

inimfon.ekpenyong@advocaat-law.com



FAVOUR ODUNOWO

favour.odunowo@advocaat-law.com

LAGOS OFFICE

13 Norman Williams Street
Off Keffi Street, Ikoyi
Lagos Nigeria

ABUJA OFFICE

Nigerian National Merit Award House Enspire
1st Floor Room 3
Plot 22 Aguiyi Ironsi Way Maitama Abuja
Nigeria

CALABAR

Akom Building
15 Murtala Mohammed Highway Calabar
Cross River
Nigeria

TELEPHONE: (LOS)+234 02014547932 (ABJ)+234 8105340496

EMAIL: info@advocaat-law.com

WEBSITE: www.advocaat-law.com