Universidad Católica del Norte

DERECHO UCN FACULTAD DE CIENCIAS JURÍDICAS

ASSISTANCE TO DOMAIN NAME HOLDERS

# FREQUENTLY ASKED QUESTIONS: DOMAIN NAME DISPUTES


**Humberto Carrasco-Blanc**

**José Sánchez-Oyarzún**

**Kathryn A. Kleiman**

**American University**

**Margarita Valdés-Cortés**

**Javier Maestre-Rodríguez**

**Chris Reed**






DERECHO UCN FACULTAD DE CIENCIAS JURÍDICAS
ASSISTANCE TO DOMAIN NAME HOLDERS
https://repositorio.ucn.cl/handle/20.500.14729/10339

# FREQUENTLY ASKED QUESTIONS: DOMAIN NAME DISPUTES

**Humberto Carrasco-Blanc**
https://orcid.org/0000-0002-1034-7521
Universidad Católica del Norte - https://ror.org/02akpm128

**José Sánchez-Oyarzún**
Universidad Católica del Norte - https://ror.org/02akpm128

**Kathryn A. Kleiman**
https://orcid.org/0009-0009-8725-0064
American University - https://ror.org/052w4zt36

**Margarita Valdés-Cortés**
Universidad de Chile - https://ror.org/047gc3g35

**Javier Maestre-Rodríguez**
Maestre Abogados

**Chris Reed**
https://orcid.org/0000-0002-9124-5489
Queen Mary University of London - https://ror.org/026zzn846

Frequently Asked Questions: Domain name disputes

Work Coordinator: Humberto Carrasco-Blanc

https://repositorio.ucn.cl/handle/20.500.14729/10339

Facultad de Ciencias Jurídicas

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

You are free to copy, redistribute, and adapt the material, even for commercial purposes, provided that appropriate credit is given and any changes made are indicated. More information: https://creativecommons.org/licenses/by/4.0/

Universidad Católica del Norte. https://ror.org/02akpm128

Published in Coquimbo, Chile, 2026.

Departamento de Ciencia Abierta y Cultura Científica.

This is a derivative work of: *Domain name disputes: Understanding the problem*. https://doi.org/10.22199/ADNH001

**Associated with this work, the following materials are available (please click the links below to access them):**

- a detailed study guide
- an audio recording,
- a video presentation,

## Acknowledgements:

This work was supported by the ICANN Grant Program through the project "Assistance for Domain Name Holders in ICANN's Uniform Dispute Resolution Policy Procedures", implemented by Universidad Católica del Norte.

The opinions and interpretations expressed in this publication are those of its authors and do not represent ICANN's official policy or position.

**Legal disclaimer:** This document is provided for educational and informational purposes only. Its content does not constitute legal advice or replace an assessment of the specific circumstances of a case by a qualified legal professional. Applicable procedures, deadlines, and rules should be verified against current official sources.

**Abstract**

This Frequently Asked Questions (FAQ) document complements *Domain Name Disputes: Understanding the Problem* by offering concise and accessible clarifications of key technical and legal concepts addressed in the main resource. Organized in a question-and-answer format, it explains how Internet addressing functions, why domain names have economic and reputational value, and how abusive online practices are regulated through international administrative mechanisms. The FAQ highlights the role of ICANN, accredited dispute-resolution providers, and the criteria applied in assessing bad faith, translating complex regulatory principles into clear guidance. As a support tool, it reinforces understanding, resolves common doubts, and strengthens foundational knowledge necessary for engaging with digital governance frameworks.

**Keywords:** FAQ; legal literacy; domain name system; ICANN; cybersquatting; bad faith; online governance; dispute resolution mechanisms; digital regulation; educational support material.

## AI Use Statement

In the preparation of this work, artificial intelligence tools such as Gemini, ChatGPT, NotebookLM, and Claude were used to support tasks including the improvement of paragraph drafting, topic research, and the development of summaries, among other uses. In addition, the final version underwent an AI-assisted adversarial audit: Claude checked part of the claims against accessible primary sources and proposed corrections, and ChatGPT independently reviewed that work. This audit does not constitute an exhaustive verification of all sources and claims. These outputs were reviewed more than twice by people, who appear as the authors, and therefore all decisions regarding content, legal interpretation, argumentative structure, and conclusions rest entirely with them, who assume full responsibility for the accuracy and rigor of the work. No sensitive or confidential information was entered into the platforms used, and each generated response was critically reviewed before being incorporated into the document.

# Table of Contents

**What is the Internet and why are domain names important?** ..... 6
**What types of conflicts can arise around domain names?** ..... 6
**How were these disputes regulated before the existence of UDRP and ICANN?** ..... 6
**What is ICANN and what is its role in resolving domain name disputes?** ..... 7
**What is the Uniform Domain Name Dispute Resolution Policy (UDRP)?** ..... 7
**What providers are there for UDRP dispute resolution and what are their differences?** ..... 7
**What does "bad faith" mean in the context of domain name disputes under the UDRP?** ..... 8
**Why is it crucial to understand how DNS and domain names work for internet users?** ..... 8

## What is the Internet and why are domain names important?

The Internet is a vast global network of interconnected computers that send and receive information continuously. For these computers to communicate effectively, systems and protocols are used, such as the Internet Protocol (IP), which uses numerical addresses (IP addresses) to identify and locate each device on the network. However, these IP addresses are difficult for users to remember. This is where domain names come into play, which are easy-to-remember alphanumeric addresses (e.g. www.harrods.com) that the Domain Name System (DNS) translates into the corresponding IP addresses. In essence, the DNS functions as a "phone book" for the Internet, allowing users to access websites without memorizing complex numbers. These names are not only a technical tool, but also crucial digital assets that represent brands, reputations, and business models.

## What types of conflicts can arise around domain names?

With the exponential growth of the Internet and the value that domain names have acquired, various abusive practices have emerged, many of which are related to intellectual property. The main ones are:

- **Cybersquatting:** It consists of registering a domain name identical or very similar to a recognized trademark, with the intention of later selling it to the legitimate owner of the trademark or taking advantage of its reputation. WWF's case against a cybersquatter who tried to sell the domain www.worldwrestlingfederation.com is a clear example.

- **Typosquatting:** Involves registering domain names with intentional typos that resemble well-known trademarks. The goal is to divert traffic from users who make mistakes when typing the address, as seen in the case of Calvin Klein against "calvjinklein.com."

- **Phishing:** It is a criminal practice where fake websites or emails are created that imitate legitimate entities (banks, companies, etc.) to deceive users and obtain sensitive personal information, such as bank details or passwords. The case of Chime Financial vs. C.S., where the official website of the financial institution was copied, illustrates this modality.

- **Reverse Domain Name Hijacking** (RDNH): Unlike the practices above, this is an abuse of the dispute resolution procedure itself, not of a domain name: using the UDRP in bad faith to attempt to deprive a registered domain-name holder of a domain name (Rules, paragraph 1)—for example, by filing a complaint knowing that it has no legitimate grounds to succeed.

These conflicts demonstrate how a domain name can be used unfairly or illicitly, causing commercial, reputational or even legal damage.

## How were these disputes regulated before the existence of UDRP and ICANN?

Prior to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998 and the Uniform Domain Name Dispute Resolution Policy (UDRP) in 1999, there were significant loopholes in domain name regulation. Emblematic cases of the 1990s, such as registration of http://panasonic.com/panavision.com and deltaairlines.com, well-known trademarks registered as domain names, highlighted this lack of regulation. These conflicts, while often resolved through settlements or court litigation, anticipated the urgent need to establish clear rules and efficient

mechanisms to quickly and efficiently protect against clear violations of trademark rights in the digital environment and avoid consumer confusion, a fundamental objective of trademark law.

## What is ICANN and what is its role in resolving domain name disputes?

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization created in 1998 at the initiative of the United States government. Its primary role is to coordinate, at the global level, the Internet's systems of unique identifiers—domain names, IP addresses and protocol parameters. ICANN is critical to the stability, security, and functioning of the Internet.

With respect to dispute resolution, ICANN is responsible for establishing procedures for addressing domain name disputes. On 26 August 1999, it adopted the Uniform Domain Name Dispute Resolution Policy (UDRP), a global regulatory framework, as its first "consensus" policy for generic top level domains that it manages and oversees, including .com, .org and .net. Under this agreed-upon policy, ICANN approves dispute-resolution service providers, which administer the proceedings under the Policy and the Rules.

## What is the Uniform Domain Name Dispute Resolution Policy (UDRP)?

The UDRP (Uniform Domain Name Dispute Resolution Policy) is a global regulatory framework established by ICANN in 1999 to resolve conflicts related to domain names, especially those involving cybersquatting, typosquatting, and phishing. This policy seeks to offer an agile and efficient administrative process to protect the legitimate rights of trademarks.

Under the UDRP, proceedings are administered by approved providers (such as WIPO, Forum, ADNDRC, CAC and CIIDRC), which apply the guiding principles of the policy, although they may incorporate complementary rules on administrative or technical aspects. The first case resolved under the UDRP was that of the World Wrestling Federation (WWF) in 2000, a clear example of cybersquatting.

## What providers are there for UDRP dispute resolution and what are their differences?

ICANN approves several providers to administer UDRP cases. The current providers are:

- **WIPO Arbitration and Mediation Center (WIPO):** Multilingual online filing and a searchable database of decisions.
- **FORUM (formerly National Arbitration Forum):** UDRP provider based in the U.S.; also administers related policies (e.g., URS).
- **Asian Domain Name Dispute Resolution Centre (ADNDRC):** Asia-focused network (offices in Beijing, Hong Kong, Kuala Lumpur, Seoul) offering multilingual handling and regional familiarity.
- **Czech Arbitration Court (CAC):** EU-based provider with a fully online platform (ADR.EU).
- **Canadian International Internet Dispute Resolution Centre (CIIDRC):** ICANN-approved provider offering online filing tools and case access.

All providers apply the **same UDRP Rules**, plus their **own Supplemental Rules**. What differs in practice are platform features (e-filing and search tools), panelist rosters, languages offered, typical timelines, and **fee schedules**. Choice of provider often turns on the case language, desired panel expertise, filing interface, and budget.

### What does "bad faith" mean in the context of domain name disputes under the UDRP?

"Bad faith" is one of the fundamental pillars of the UDRP and a key criterion for determining whether a domain name should be cancelled or transferred. It refers to the intent to harm, deceive, or take advantage of a third party's reputation through the registration and use of a domain name; the UDRP requires bad faith in both.

Bad faith is not presumed, but it can be inferred from certain circumstances or behaviors of the domain holder. Examples of bad faith include:

- Offering to sell the domain name to the trademark owner for an excessive price (cybersquatting).
- Registering multiple domain names that are confusingly similar to third-party trademarks.
- Using the domain to divert traffic, confuse consumers, or facilitate fraudulent activities such as phishing.

Proving bad faith is crucial for a UDRP complaint to succeed, as it allows differentiating between legitimate and abusive uses of a domain name.

Clear defenses: The ICANN Community adopted clear defenses that a domain name registrant may show. The Policy (paragraph 4(c)) identifies circumstances through which a registrant may demonstrate rights or legitimate interests in the domain name, including:

- before any notice of the dispute, registrant made use of, or demonstrable preparations to use, the domain name in connection with a bona fide offering of goods or services;
- as an individual, business, or other organization, the registrant is commonly known by the domain name, even if no trademark or service mark rights have been acquired.
- registrant is making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

### Why is it crucial to understand how DNS and domain names work for internet users?

Understanding how the Domain Name System (DNS) works and the importance of domain names is essential to be an active and secure player in the digital environment. Domain names are more than just technical addresses; They are valuable digital assets that represent the identity and reputation of individuals, businesses, and organizations online.

Knowing these basics allows users to:

- **Protect their interests:** Understanding the risks associated with abusive practices such as cybersquatting, typosquatting, and phishing helps protect brands, reputations, and personal data.
- **Actively participate:** For those who want to create a website or manage a domain name, knowledge of DNS is essential for its correct configuration and use.
- **Contribute to a safer Internet: By** understanding how domains can be used for malicious purposes, users can take precautions and contribute to a fairer and more transparent online environment.

In short, this knowledge not only helps protect one's own interests, but is also key to navigating and operating the Internet in an informed and responsible manner.

Universidad Católica del Norte

DERECHO UCN FACULTAD DE CIENCIAS JURÍDICAS

ASSISTANCE TO DOMAIN NAME HOLDERS

**To cite the work in APA 7.**

Carrasco-Blanc, H., Sánchez-Oyarzún, J., Kleiman, K. A., Valdés-Cortés, M., Maestre-Rodríguez, J., & Reed, C. (2016). *Frequently Asked Questions: Domain name disputes.* Ediciones Científicas Norte. https://repositorio.ucn.cl/handle/20.500.14729/10339