The UDRP Process

Be prepared to be prosperous

Introduction to the UDRP Process

In the last twenty-five years the number of Uniform Domain Name Dispute Resolution Policy (UDRP) cases handled by the World Intellectual Property Organization (WIPO) – the global leader, has risen by over 300% to a record of 6,282 in 2025, reflecting both the continued growth in cases of cybersquatting, and the resilience and effectiveness of UDRP as the only global domain dispute mechanism. Without such a global mechanism to address domain name-related trademark infringement, most cross border domain name disputes would simply go unresolved, resulting in harm to brands and consumers, because litigation in multiple jurisdictions is impractical.

The UDRP still works remarkably well when it is used for what it was designed for, a point emphasized by WIPO's Head of Internet Dispute Section Brian Beckham when he recently spoke to a room full of brand holders and IP counsels in London. It addresses cases of bad faith domain name registrations specifically targeting trademarks. Success rates for complainants are very high, which sometimes prompts criticism that the system is biased, but Beckham reminds us of all that the policy is intentionally calibrated to address a problem faced by brand owners and that the three elements are spelled out, in black and white. Those three elements are:

- That the disputed domain name is identical or confusingly similar to a trademark or a service mark in which the complainant has rights;
- The respondent has no rights or legitimate interests in respect of the domain name; and
- The domain name has been registered and is being used in bad faith.

Where complainants understand those three elements and do their basic homework, they should be able to predict the outcome. Many experienced UDRP practitioners have 100%-win rates on well chosen cases, a fact borne out by Com Laude's perfect success rate stretching back over 23 years across in more than 750 dispute cases.

Common misunderstandings on filing UDRP complaints

There are two areas, based on Beckham's experience at WIPO where UDRP is commonly misunderstood or misused. The first is in so-called 'Buyer's remorse' cases where brand owners balk at the price of a domain name being offered on the secondary market. Instead they decide to file a UDRP instead of negotiating with the seller, who is motivated to sell the domain name. This approach sometimes backfires as it could lead to a reverse domain name hijacking (RDNH) decision, hardened positions and lead to a higher price being set by the registrant.

...the message is clear: those who understand both the strengths and limits of the UDRP, and who adapt to these refinements, will be best placed to protect their organisations in an increasingly complex domain name environment.

The second, is becoming more common unfortunately as filers of cases look to use shortcuts in the preparation. The old adage of failing to prepare means you prepare to fail is never truer in this sense. Beckham cited a rise in complaints being "phoned in" or cases that are all treated the same even when the facts may be more complex. Those are the ones poorly drafted, template driven filings that ignore obvious evidence of legitimate interest revealed after GDPR era disclosure. Or they may omit basic exhibits, provide incomplete or disorganised document packs or even leave the wrong domain or policy name in from template documents or previous cases. These trigger panel frustration, RDNH findings, and occasionally denials in cases that might have been straightforward wins had the time been taken to properly research and file the necessary evidence and exhibits with the complaint

The changing nature of the domain infringement landscape

The nature of disputes has changed over the years. A significant number of disputes used to be related to infringing domain names that were hosting pay per click parking, focusing on monetisation of the brand holder's intellectual property. Over time these have become less frequent reasons for a complaint being filed on particularly as search platforms have adjusted their algorithms to defocus on this type of web content, and thus make those domain names less attractive to cybersquatters seeking a fast buck.

Today, phishing, fake invoice scams, advance fee fraud and credential harvesting are much more prevalent, often using domains that mimic corporate subdomains like [brand]careers, [brand]HR, or [brand]recruitment. One tactic that Beckham has seen at WIPO is where brand infringers use tools to discover internal subdomains being used, then register similar domain names to host fake login portals and harvest data for fraudulent purposes.

Beckham has also seen a rise in cases where an inadvertent lapse in the renewal of key domains. Drop domain names can be hard to recover under the UDRP when the mark is descriptive, and this domain portfolio hygiene, such as ensuring those most important names are registry locked and on auto-renewal, remains critical.

The WIPO and ICA Review

As part of ongoing reviews into Rights Protection Mechanisms (RPMs), and to give ICANN a set of guidelines to develop their own review of RPMs, The Internet Commerce Association (ICA) and WIPO started collaborating on a joint review of the UDRP process. This two-year project finally delivered their final findings, a set of 25 mostly light-touch pragmatic recommendations to ICANN in December 2025.

Beckham describes this collaboration as unprecedented given historic tensions between IP interests and professional domain investors, which is why both parties approached their recommendations with the objective to preserve the core effectiveness of the UDRP while tidying operational and procedural issues.

New WIPO Services and Operational Changes

Aside from the recommendations from the joint review, WIPO are looking to introduce some new services and operational changes themselves in the coming months, including a premium-fee fast track process that will aim to make decisions within 30 days of filing a complaint.

Another notable change reflects cases filed as a "John Doe" case but terminated prior to formal commencement. Because GDPR driven redaction forces most complaints to be filed initially against unknown respondents, where a filed complaint sometimes reveals underlying registrant data that makes a previously unknowable defence of the case obvious - e.g., the underlying registrant is a business or individual whose company or surname is reflected in the domain name. In those scenarios, the complainant must file in the dark and will want to withdraw the case for a refund of all but a small ($100) admin fee.

This is intended to break the current logjam where registrars often refuse to disclose data directly and tell rights holders to "file a UDRP or go to court," even though ICANN's Temporary Specification clearly contemplates cybersquatting cases as a legitimate interest basis for disclosure (the UDRP is also contractual). Many of these cases would not have been filed in the past or would have been negotiated based on public WHIOS information.

One of the other recommendations from the UDRP review was the idea of blacklisting of proven bad faith typos or misspellings of marks following successful UDRP decisions, modelled on a (former) prohibition on misspellings policy used in Australia. Under such a system, domains found to be abusive would be blocked at the registry level from re registration, subject to a mechanism for third parties with legitimate interests to apply for the domain name to be unblocked and registered. In Beckham's eyes, he believes this would meaningfully reduce costly defensive registration portfolios without materially harming registry or registrar revenues and could generate significant goodwill for ICANN and its contracted parties if adopted.

What this means for rights holders

In the changing domain infringement landscape UDRP remains a uniquely effective global tool for tackling clear-cut, bad-faith domain name abuse, one that demands informed and disciplined use by brand owners and their advisors. By avoiding "buyer's remorse" complaints, investing time in well-prepared filings, and maintaining robust domain portfolio hygiene, rights holders can continue to secure consistently favourable outcomes while minimising the risk of reverse domain name hijacking or adverse decisions.

The joint WIPO–ICA review, published in December 2025 and WIPO's forthcoming operational enhancements show that the UDRP system is still evolving in a pragmatic, light-touch way to address modern threats such as phishing and GDPR-era data-access challenges without undermining the policy's core architecture. For in-house and external counsel, the message is clear: those who understand both the strengths and limits of the UDRP, and who adapt to these refinements, will be best placed to protect their organisations in an increasingly complex domain name environment.

ComLaude

Contact us today for a confidential discussion about your domain dispute or portfolio protection needs.