Markmonitor™

# UDRP for Brand Protection

## Gain Control of Domain Names Using Your Marks That Are Registered by Third Parties

**For Additional Information, Contact Your Account Manager or Visit markmonitor.com**

# UDRP: Brand Protection Across gTLDs - Gain Control of Domain Names Registered in Bad Faith

## The UDRP: An Executive Overview

If a third party registers a domain name incorporating your trademark in bad faith under a generic Top-Level Domain (gTLD), the Uniform Domain-Name Dispute Resolution Policy (UDRP) provides a structured brand protection mechanism to recover that domain.

The UDRP Is:

- An administrative process
  - Not an expensive negotiation tactic or litigious process
- A defined framework adopted by ICANN in 1999
  - Registrars are bound to it as per their registrar accreditation agreements
- Applicable to most gTLDs
- Designed to combat the brand risks 3rd party registrations may introduce, like:
  - Phishing, impersonation, recruitment fraud, counterfeit commerce
- One of the most reliable domain recovery mechanisms available to brand holders
- More likely to have a favorable outcome for brands when they consult with a partner like Markmonitor for guidance and filing

## The Intersection of Enterprise Domain Strategy and UDRP

A domain name dispute does not exist in isolation. Online brand protection measures intersect with:

- Portfolio governance
- Defensive registration or blocking strategy
- DNS configuration
- Monitoring and detection programs
- Fraud response coordination
- Registry and registrar escalation pathways

Treating the UDRP as a standalone tactic for domain name recovery ignores the operational ecosystem in which online brand abuse occurs. A progressive escalation pathway based on risk severity, registrar cooperation, and jurisdiction could look like:

- Cease & Desist Letters: Legal letter demanding removal
- Takedown: Abuse complaint to registrar, registry, or host; fastest for clear-cut infringement
- UDRP/DRP: Dispute resolution through ICANN; lower cost than court, 45–60-day timeline
- Acquisition: May be the most cost-effective, quickest and pragmatic option in some cases; can be open or anonymous
- Litigation: Most expensive but strongest remedy for serious fraud or repeat offenders; option of last resort

### Why Enterprises Engage Markmonitor for UDRP Proceedings

Markmonitor operates as a corporate domain registrar serving global enterprise portfolios.

That matters for three reasons:

1. We understand your domain architecture and portfolio governance models
2. We integrate enforcement into the portfolio strategy best suited for your brand
3. We coordinate across monitoring, registry interactions, DNS configuration, and escalation channels

UDRP is deployed as part of a structured brand protection strategy tailored to your specific needs that may also include cease-and-desist correspondence, registry engagement, defensive registrations, and technical controls.

At Markmonitor, our objective is never to simply win a UDRP filing: it is to remove abusive infrastructure and reinforce perimeter control so your brand remains protected online.

**Enforcement Environment: Impact of Data Privacy Restrictions**

Over the past decade, access to accurate registrant data has become more difficult due to global privacy regulations, including the GDPR and related frameworks. This data-privacy-first approach, while understandable for end users, makes brand protection challenging for an enterprise to undertake on its own.

Practical impact:

- WHOIS records frequently masked or redacted
- Registrant identity often undisclosed
- Direct contact unreliable
- Informal recovery efforts are frequently ineffective

As registrant anonymity has increased, formal administrative remedies have become more central to enforcement strategy.

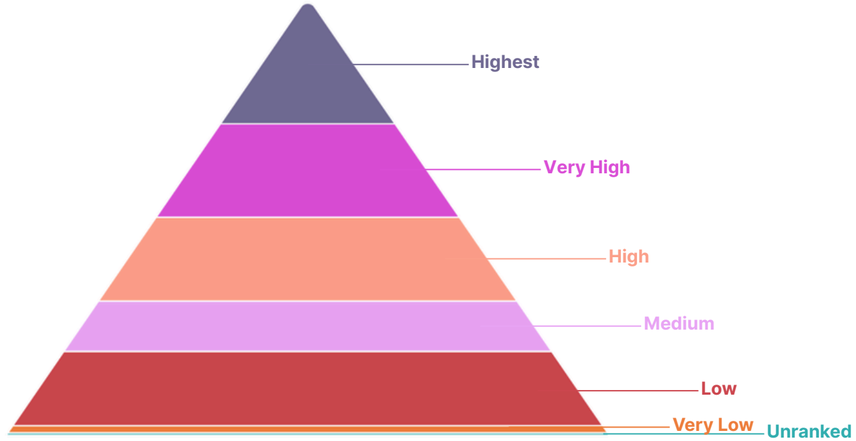
**Execution Risks in UDRP Proceedings**

Unsuccessful complaints typically result from:

- Incomplete evidence development
- Insufficient documentation of trademark rights
- Weak articulation of bad-faith use
- Procedural non-compliance
- Misalignment with broader portfolio strategy

As the UDRP is procedural, success depends on disciplined preparation and integration with brand governance. Allow us to help your brand successfully recover your domain names today.

## Threat Distribution




## Insights

- **2** new domain names were detected in the last month
- **171** domain names are ranked in the highest threat category
- The most ccTLDs were registered in the **co.nz,it** space in the past 12 months
- We found **1040** active domain names in total related to this brand
- **223** domain names are configured with MX records
- The domain **buylavazzacoffee.com** scored risk has increased the most within the last month

**When to Initiate a UDRP Proceeding with Markmonitor**

Consider pursuing a UDRP filing to protect your brand when:

- The domain is registered under a covered gTLD
- Your trademark rights are established and defensible
- Evidence of bad-faith registration and use exists
- The harm is material or ongoing
- Informal resolution is impractical

In these circumstances, partnering with an online brand protection expert like Markmonitor to file a UDRP provides a structured path to regaining control of your name.

**UDRP: Regaining Control of Your Mark in Domain Registrations Is a Governance Decision**

A successful UDRP results in:

- Transfer of the domain to your control, or
- Cancellation of the registration

Allowing an abusive domain incorporating your trademark to remain active carries measurable fraud, reputational, and operational risk.

UDRP remains one of the most effective administrative mechanisms for regaining control of such domains under gTLDs.

When executed with procedural rigor and integrated into an enterprise domain governance strategy, it supports online brand protection efforts.

Markmonitor supports global brands in evaluating, preparing, and executing UDRP proceedings as part of a coordinated domain and brand protection strategy.

**For Additional Information, Contact Your Account Manager or Visit markmonitor.com**