Articles + Publications | August 19, 2025

Your Brand, Their Bait: Fighting Impersonation in the Age of Digital Deception

WRITTEN BY

H. Straat Tenney | Emma Bennett

Businesses invest an immense amount of time, effort, and financial resources into building their brand identity and overall cultivating a strong foundation of consumer trust. This trust is not only a cornerstone of a brand's reputation but is also a critical component of its long-term success in the marketplace. However, with the rise of phishing attacks, a brand's trust can be quickly weaponized against unsuspecting customers when bad actors create fraudulent websites or send phishing emails impersonating an authentic business. These deceptive tactics often involve using the company's trademark, trade dress, and copyrighted images to appear legitimate, tricking unsuspecting customers into divulging their personal and sensitive information.

Your Brand Is on the Line

The Federal Trade Commission (FTC) recently unveiled its August Data Spotlight, highlighting a concerning trend: reports of impersonation scams resulting in significant financial losses have quadrupled since 2020.[1] Specifically, the number of reports increased from roughly 1,800 in 2020 to exceeding 8,000 in 2024.[2] This increase underscores the growing threat of impersonation to consumers themselves.

Approximately 28% of impersonation scams[3] originate from interactions through online platforms and email communications, where impersonators can craft fraudulent emails or websites that mimic the appearance and functionality of legitimate businesses. And while the FTC's report focuses on the ramifications of impersonation for consumers and outlines measures that individuals can adopt to protect themselves, it leaves open the question of what companies can do when targeted by these bad actors. One significant challenge with impersonators is their anonymity. The privacy mechanisms embedded in the domain registration process allow registrants to conceal their identities, making it difficult to determine who is responsible for the impersonation. This obfuscation poses a barrier to pursuing legal action, since starting formal litigation requires knowing the party to be sued.

Reeling Back in Your Reputation

Nonetheless, businesses have an effective tool to combat brand impersonation — their intellectual property.

I. Uniform Domain-Name Dispute-Resolution Policy

The Uniform Domain-Name Dispute-Resolution Policy (UDRP) provides a structured mechanism for trademark owners to challenge domains that mirror or closely resemble their trademarks. To successfully employ UDRP as an enforcement tool, the trademark owner must demonstrate three key elements:

1. An identical or confusingly similar domain name;
2. A lack of legitimate interest in the domain name; and
3. Bad faith registration and use.

While the UDRP process involves drafting a complaint and paying a filing fee, it remains less formal, quicker, and cheaper compared to federal trademark litigation. Given the nature of impersonators, they often do not respond to UDRP proceedings, streamlining the process for rightful trademark holders to reclaim rights in the infringing domain.

II. Digital Millennium Copyright Act

In situations where a fraudulent entity isn't explicitly using your trademark but has essentially duplicated a website under a different domain name, businesses may have recourse under the Digital Millennium Copyright Act (DMCA). If images or content from the authentic website are mirrored on an impersonating site, the DMCA makes it considerably easier for website owners to issue takedown requests to service providers, website operators, search engines, or registrars (discussed more below). These providers are often reluctant to wade into arguably questionable trademark disputes but will act swiftly to remove infringing copyrights. Additionally, utilizing tools like Google image search can be an effective strategy to identify infringing uses. Overall, relying on copyright will help ensure the removal of impersonating websites without the need for intricate comparisons between trademarks or commercial offerings.

III. Takedown Request to Domain Registrar for Repeat Impersonations

Submitting takedown requests to the registrar of the impersonating domain can be a cost-effective and fast option when you are dealing with repeat impersonations. This option generally involves reporting the infringing site directly to the registrar. This process has varying timelines and procedures depending on the registrar involved. Some registrars have established formal forms and guidelines for takedown requests, while others might just require an email to their legal team.

Regardless of the registrar's specific process, the most successful takedown requests typically include clear evidence of rights in its intellectual property and documentation of the malicious intent or bad faith use of the domain, such as examples of the phishing or impersonation activity.

When submitting takedown requests, it's important to remember that the individuals reviewing these requests are typically knowledgeable and aware of intellectual property issues. If your demands are excessive or unreasonable, or if your client's rights are unclear, it could negatively affect the perception of your client or brand. Registrars often opt to suspend domains rather than transfer them in response to takedown requests, so it's crucial to be mindful of specific registrar policies regarding the re-release of suspended domains, as it may affect your takedown strategy.

The best results often come from combining UDRP or DMCA with takedown requests. Successful UDRP decisions or DMCA requests lend credibility to subsequent takedown requests, prompting registrars to take reports of abuse more seriously. This integrated approach strengthens the defense against repeat impersonation and domain abuse.

Casting a Wide Net of Protections

For both UDRP and takedown requests, having a registered trademark, whether with the U.S. Patent and Trademark Office or in foreign countries, streamlines UDRP proceedings because trademark registration creates a legal presumption that the mark is valid, that you own the trademark, and have the right to use the mark. A registration provides a solid legal basis for enforcers to quickly act upon infringement and impersonation claims.

Moreover, when encountering repeated impersonation, additional strategies can bolster your defenses. Domain watch services and real-time notifications are invaluable tools that monitor domain activity, alerting you to new registrations that mimic or infringe upon your trademark. Defensive domain registration is another effective measure. By preemptively buying domains that closely resemble your brand, you can deny impersonators the opportunity to exploit them.

Overall, safeguarding brand identity in the digital landscape demands a strategic blend of proactive and defensive actions. Using a trademark and copyright as the legal foundation, businesses are likely to have success with both the UDRP or DMCA and takedown requests to fight impersonation. These actions not only mitigate risk for consumers, but also prevent impersonators from causing lasting reputational harm — especially when they already have a hook in your brand.

---

[1] https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-data-show-more-four-fold-increase-reports-impersonation-scammers-stealing-tens-even-hundreds.

[2] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings#ftn3 at n.3.

[3] *Id.* at n.2.

RELATED INDUSTRIES + PRACTICES

- Domain Name Litigation + UDRPs
- Intellectual Property
- Privacy + Cyber
- Trademark + Copyright