



CLIENT ALERT

December 3, 2021

1

BRAND PROTECTION AND FIGHTING FAKES ONLINE

by John L. Krieger and Tenesa S. Powell

The shift to online marketplaces has created an incredible boom for some, and significant loss to others. Branding has become more important than ever, particularly in developing an online presence through search engines, various online platforms, and social media. Further, the rise of the “influencer” has opened additional opportunities to deliver brands and products to targeted demographics. However, these great advances also come with some disadvantages that can become quite onerous and problematic. Fakes and counterfeits are part of these unwelcome advances, and seem to have come out of the “dark back alleys,” finding a “legitimate” storefront on various websites and platforms. Unfortunately, a brand owner must continually “police” its marks or suffer a loss in value and recognition, and, potentially, loss of the brand.

The ever-expanding internet presents a daunting task to any brand owner trying to police its marks. Due to the protections extended to “internet content providers” under Section 240 of the Communications Decency Act, most websites and platforms are absolved of liability for infringing third-party content. As a result, the burden to police falls on the mark owner. There are a number of companies and law firms that are able to harness software and manpower to scour the internet on behalf of brand owners, but those routes can be cost-prohibitive for some. However, there are a number of easy steps any brand owner can use to protect its brand online.

Online Marketplace Protection

Nearly every mainstream marketplace and social media platform has Acceptable Use Policies, which provide procedures for reporting intellectual property infringements. Despite the proliferation of counterfeit goods and fake accounts, there are surprisingly few companies that offer monitoring services. The most prominent are Amazon and Facebook.

The Amazon Brand Registry (“The Registry”)¹ is a free service, which allows the brand owner to search for content using images and keywords and report violations. In order to utilize The Registry, the brand owner must have a federally-registered trademark that appears on products or packaging. The Registry requires verification of the rights by the brand owner listed with the USPTO on the registration in order to create the account. The owner must apply for registration and will need to provide the trademark registration number, product categories, and a list of countries where products are manufactured and distributed. In addition to streamlining the brand owner’s proactive monitoring, The Registry uses the information provided by the brand owner to proactively remove suspected infringing listings. According

to Amazon, The Registry’s automated screening process stopped more than 10 billion suspected problematic listings.

In order to take advantage of Facebook’s free monitoring service, the brand owner must apply for access to Facebook’s tool and must have a registered trademark.² The program is limited to searching ads, marketplace posts, and group sale posts and does not cover copyright or unregistered trademarks.

Third-party services such as those offered by Corsearch or MarkMonitor, allow a brand owner to not only monitor infringing uses, but also identify counterfeits and lookalike products.

Combatting Cybersquatters

While cybersquatters have been around for decades, cybersquatters in the 2020s are amping up their game by leveraging counterfeit websites to perpetrate fraud in the name of the brand owner. While “run of the mill” cybersquatting undoubtedly damages brands and goodwill, adding a counterfeit website gives the cybersquatter an additional layer of perceived legitimacy. This perceived legitimacy ups the confusion ante and exposes consumers to fraud and identity theft, all at the expense of the brand owner’s reputation.

For example, a financial investment firm that is subject to various regulatory bodies was the target of cybersquatting involving both an infringing domain name and a counterfeit website. The counterfeit website went so far as to include the same physical address and business license information for the investment firm. At least two consumers lost thousands of dollars each, not only damaging the investment firm’s brand and goodwill, but also its reputation with regulatory authorities. In another case, a well-known sports exhibitor encountered similar cybersquatting plus counterfeit website, which purported to offer streaming services of its events. The counterfeit website included nearly identical photos and text to those used by the brand owner on its website, which caused greater consumer confusion. Here again, innocent consumers provided private financial information believing they were receiving legitimate services from the brand owner, when they were not.

With these higher-stakes infringers looking to exploit consumers at a brand owner’s expense, it is even more imperative brand owners take proactive measures to monitor domain name registrations in order to stop infringers before they have an opportunity to start. One example is Brand Monitor, offered through DomainTools.³ For less than \$1,000 per year, Brand Monitor will allow a brand owner to monitor domain

¹ <https://brandservices.amazon.com/?ld=BRUSNF> (last visited Oct. 13, 2021).

² <https://www.facebook.com/help/contact/423912757973851> (last visited Oct. 13, 2021).

³ Neither the authors nor their firm has received any financial incentive for identifying any product or service in this article.

registrations for brand names and common variants. CheckMark Network offers similar domain monitoring services that include identical or confusingly similar domain names, prefix, suffix, or mid-word occurrences, and uses a typo-squatting algorithm to maximize monitoring.

While a brand owner can go after an infringing domain name using the Uniform Dispute Resolution Policy (“UDRP”), the UDRP does not have a mechanism to immediately take down a counterfeit website.⁴ In cases where a counterfeit website needs to be brought down immediately, the brand owner should consider filing a cybersquatting lawsuit in federal court and seek an immediate *ex parte* temporary restraining order requiring the domain name registry or registrar to disconnect the website from the domain name.

Using Copyright Law to Fight Fakes

Copyright law also provides an avenue of protection for brand owners. Oftentimes, infringers and/or counterfeiters will steal images from the brand owner’s website and then use those images to promote and sell counterfeit goods. These images are generally high quality and a great representation of the brand, which is why they are used by infringers and counterfeiters. Moreover, the images can be used to “pass off” oneself as being legitimately connected to, affiliated with, or endorsed by the brand owner when they are not. By tracking its own images across the internet, the brand owner has a more targeted approach as opposed to simply trying to manually input search terms in a search engine. There are several free or low-cost software available to reverse search images on the internet. For example, YouTube has a fairly robust free copyright infringement monitoring program called Content ID.⁵ These tools can be invaluable. And, where feasible, brand owners may want to consider hiring a person(s) whose sole purpose is to employ these tools to scour the internet for infringements.⁶

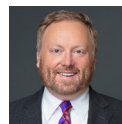
The advantage of employing an online copyright search for brand images is that a copyright registration is not required. Ownership in copyrights vests upon creation of the work.⁷ Therefore, the mark owner can pursue enforcement without the need to fulfill an extra step. The Digital Millennium Copyright Act (“DMCA”) requires website owners to create an ability for a brand owner to petition the site to take down an infringing work in order to avoid liability for the same.⁸ Most websites and online market platforms have online dedicated DMCA take-down forms/submissions to make it easier on the brand owner. The brand owner then needs only make an affirmative sworn statement that the image belongs to it and it is being used by the infringer or counterfeiter without permission. DMCA take-down notices can be fairly effective and removing infringing content quickly. The DMCA is best used in cases of a clear-cut obvious case of copying – where the image is identical to and lifted from the mark owner’s website.

Additionally, in lieu of pursuing full-blown federal copyright litigation, the recently enacted Copyright Alternative in Small-Claims Enforcement Act of 2019 (“CASE Act”), which becomes effective December 27, 2021, offers a great alternative.⁹ The CASE Act established the Copyright Claims Board (“CCB”) – a voluntary administrative body, akin to the

Trademark Trial and Appeal Board, but less formal. The CCB is intended to be a vehicle for minimizing fees and costs generally associated with litigation, and has the express goal of expediting resolution. Unlike federal court, there is no requirement for the brand owner to obtain a copyright registration before instituting a CCB proceeding. Further, the Rules of Evidence do not apply, and filing fees are a fraction of federal court fees. Indeed, the Act limits the amount of damages to a maximum of \$30,000 as compared to maximum damages under the Copyright Act of \$150,000 per work. While participation is voluntary, a proceeding in front of the CCB works on an “opt-out” basis rather than an “opt-in” basis. What this means, practically speaking, is that once a rights holder initiates a claim in front of the CCB, the responding party must affirmatively disagree with proceeding in front of the CCB.¹⁰ While opponents of the CASE Act criticize this opt-out scheme as being unconstitutional based on due process considerations, the CCB is intended to provide an alternative solution to the rights owners. And, it offers the benefit that if the defendant fails to appear, the brand owner can obtain a default judgment and enforce it in federal court.¹¹

Given the increase in counterfeit websites, which are often accompanied by a domain name similar to an established brand, brand owners face increased harm to their goodwill and reputation. Brand owners should increase monitoring and vigilance in protecting their intellectual property rights. They should also take advantage of free services offered by some larger companies, such as Amazon and Facebook, and engage dedicated companies and/or employees to monitor individual websites and marketplaces for counterfeits and other infringements.

ABOUT THE AUTHORS



John L. Krieger is a Member in Dickinson Wright’s Las Vegas office. He can be reached at 702.550.4439 or jkrieger@dickinsonwright.com.



Tenesa S. Powell is Of Counsel in Dickinson Wright’s Las Vegas office. She can be reached at 702.550.4472 or tpowell@dickinsonwright.com.

⁴ A complainant’s remedies are limited to cancellation or transfer of the domain name.

⁵ <https://support.google.com/youtube/answer/2797370?hl=en#zippy=%2Cwhat-options-are-available-to-copyright-owners> (last visited Oct. 15, 2021).

⁶ *Design Basics, LLC v. Signature Constr., Inc.*, 994 F.3d 879, 882 (7th Cir. 2021) (noting plaintiff had “employees trawl the Internet in search of targets for strategic infringement suits”).

⁷ 17 U.S.C. § 201

⁸ 17 U.S.C. § 1201

⁹ H.R. 2426 – CASE Act of 2019

¹⁰ The implementing procedures for the CCB are going through the proposed rulemaking and public comment phase. For the most current status of CCB rulemaking, visit <https://www.copyright.gov/about/small-claims/related-rulemakings.html> (last visited Oct. 13, 2021).

¹¹ H.R. 2426 – CASE Act of 2019, § 1508.