

A Quick Fix for Online Trademark Infringement

Trademark infringements are pervasive on the Internet. One recent scam involves fake offers for free or discounted goods and services in exchange for posting links and “liking” something on Facebook. These scammers use the trademarks of well-known companies in a variety of industries—from airlines to restaurants—to publicize offers on websites that look legitimate when they are not. The unauthorized uses of the trademarks cause confusion among consumers and constitute trademark infringement, among other things. Companies are taking action to protect their brands from this kind of abuse.

One of the most efficient and cost-effective means of addressing these scams is by contacting the Internet service providers (ISPs) to ask them to remove the content or otherwise disable access to the sites where the infringements occur. Many ISPs have developed acceptable use policies that prohibit trademark infringement and provide for infringing material to be taken down when trademark owners report violations. This article discusses best practices for handling removal of material infringing on trademarks from websites.



The Digital Millennium Copyright Act: A Workable Framework

There is no particular trademark law that specifies how ISPs should react to notices of trademark infringement. Although the Digital Millennium Copyright Act (DMCA) has been in effect since 1998 to address copyright infringement online and the liability of ISPs hosting such content, no parallel legislation exists specifically to address these issues in the trademark area. The DMCA procedure is instructive, though, in establishing best practices for handling material that infringes a trademark.

Under the DMCA, every ISP has a duty to develop a policy and procedures for the removal of infringing material from websites it controls and operates on its servers. To comply with the DMCA, an ISP must take down infringing material upon receiving proper notice from the copyright owner. Generally, upon receiving this notice, the ISP will take down the infringing material and forward the notice to the website owner, who will then have an opportunity to present a counter-notice if it claims the material does not infringe copyright. Then, if the copyright owner does not file a lawsuit to protect his or her rights, the ISP is required

to restore the material to the website.¹

Many ISPs have voluntarily extended their DMCA policies and procedures to cover trademarks in addition to copyrights, and they will generally respond to a takedown notice based on trademark rights by either removing the infringing material or disabling the website. This became commonplace in the wake of the 2008 decision made by the Second Circuit Court of Appeals in *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 94 U.S.P.Q.2d 1188 (2d Cir. 2010). In *Tiffany v. eBay*, the Second Circuit held that ISPs charged with hosting websites that infringe on a third party's trademark rights may face liability for contributory infringement if they continue to provide server space to the infringer despite knowing about the infringement. The district court found that eBay's practice of promptly removing challenged listings after receiving notices of trademark infringement protected it from contributory liability, and the Second Circuit Court of Appeals agreed.

Identification of the Correct Internet Service Provider

The most difficult step in the takedown process often may be locating the correct ISP that is providing the hosting services and server space for the infringing site. The first step is to identify the IP address for the infringing site. The starting point should be the WHOIS record for the domain name in question. Each registrar is required to maintain a WHOIS database, and there are some websites that search WHOIS records across many registrars (www.betterwhois.com is one example). At a minimum, the WHOIS record should provide the name of the registrar of the domain name and the name of the domain server. In some cases, the registrar may also be providing the hosting services for the domain name.

The WHOIS record should also have the name and contact information for the owner of the domain name (the registrant), and the name and contact information for an administrator and technical contact person for the domain name. Because many owners of domain names are now using privacy services available through the various registrars, instead of information for an individual or a company, the WHOIS record will indicate that this information is privacy protected. The privacy services generally have terms of service that permit the name and contact information to be disclosed when infringement is alleged. For purposes of sending a takedown notice, it is not necessary to identify the website owner. It is helpful, however, to have this information to establish a pattern of infringement

perpetrated by one individual (some ISPs will disable the infringer's account in cases of repeat offenders) or to follow up with a cease-and-desist letter directly to the individual.

A Domain Information Groper (DIG) search can be conducted on the domain name in order to obtain an IP address for an infringing website.² Free DIG searches are available for individual use at www.kloth.net. Once the IP address is identified, searching the American Registry for Internet Numbers (ARIN) database at www.arin.net will provide the name and contact information for the ISP that has been assigned that particular range of IP addresses. Usually an address or e-mail address for reporting abuse is available from ARIN; however, the information available on ARIN is not always current and accurate.

Another option is to search the list of DMCA-designated agents on file at the U.S. Copyright office, available at www.copyright.gov/onlinesp/list/a_agents.html. As noted above, the DMCA-designated agent often will also be the person who will handle trademark infringement claims for the ISP, or at least the person who would be in a better position to process the notice than others in the company.

Content of the Trademark Takedown Notice

Once the proper ISP is identified, the next step is to review the ISP's trademark policies, which are frequently part of the ISP's Acceptable Use Policy (AUP), Terms of Service (TOS), or Terms of Use. Usually there will be a heading or subheading for Intellectual Property, Copyright, or Trademark Infringement. Many ISPs have simply added trademark claims under the umbrella of their DMCA policy.

As for the content of the takedown notice, if not otherwise specified in the ISP's policy, trademark owners should provide all the information typically found in a DMCA notice:

- the name, contact information, and electronic signature of the person giving notice;
- the URL of the infringing website;
- information sufficient to identify the infringing material;
- a recitation stating a good faith belief that the use of the infringing material is not authorized by the copyright owner or the law; and
- a certification under penalty of perjury that the information in the notice is accurate and that the person submitting the notice is either the copyright owner or the owner's authorized agent.

The notice should also include the basis for demonstrating trademark rights, including any registration numbers or serial numbers assigned by the U.S. Patent and Trademark Office. It is also helpful to reference the ISP's specific policy that is being violated.

Another best practice is to be sure to word the trademark takedown notice carefully so that it clearly

asserts *trademark* rights and does not run afoul of § 512(f) by citing the DMCA as the authority for the notice. To the extent the infringement entails content that infringes both trademark *and* copyright, it may be prudent to send two separate notices, one dealing just with the trademark issues and one that is strictly a DMCA notice addressing the copyright infringement.

Conclusion

Sending a takedown notice can be a quick and easy way to stop trademark infringement on a particular website. This technique is likely to be most effective against an infringer who is new to Internet marketing and lacks an understanding of the serious nature of trademark rights in the United States. When dealing with professional infringers who make their living by conducting this type of activity, it can be harder to stop them with one takedown notice; it may take several rounds of notices as well as cease-and-desist letters to obtain the desired result. As always, keeping a detailed record of the infringing websites and the steps taken against the infringers will assist if litigation becomes necessary. **TFL**

Deborah A. Wilcox is a partner and office coordinator for Baker Hostetler LLP's Intellectual Property, Technology and Media Practice in Cleveland, Ohio. She manages complex copyright, trademark, and e-commerce litigation and counsels clients on trademark and copyright registration and licensing, anticounterfeiting strategies, and digital media and advertising matters. She is currently serving as the president of the Cleveland Intellectual Property Law Association. Courtni E. Thorpe is an associate in the Intellectual Property Group at Baker Hostetler LLP in Cleveland, Ohio, where she handles disputes involving online trademark and copyright infringement, counsels clients on IP portfolio management, prosecutes trademark applications, and assists with IP litigation. © 2012 Deborah A. Wilcox and Courtni E. Thorpe. All rights reserved.

Endnotes

¹It is important to note that the DMCA is limited to copyright protection, and the law prohibits sending false notices requesting the takedown of material that is not protected by copyright or is not infringing copyright. Case law is still developing in this area, but improperly asserting trademark infringement under the DMCA might be considered an abusive copyright claim under § 512(f) of the DMCA. See *Online Policy Group v. Diebold Inc.*, 72 U.S.P.Q.2d 1200 (N.D. Cal. 2004) (sending takedown notices to ISPs when the defendant knew the material in question was not protected by copyright found to be abusive copyright claims under DMCA).

²As explained on www.kloth.net, "The DIG utility (domain information groper) is a Unix tool, which can be used to gather information from the Domain Name System servers."