



PROTECTING YOUR CLIENT'S BRANDS FROM DOMAIN NAME THEFT AND SCAMS

By Debra Y. Hughes, Esq. and David A. Bell, Esq.*

Why Should You Pay Close Attention Now to Domain Name Issues?

In short, the right domain name is prime "virtual" real estate that can leverage a company's visibility, and for this reason, domain names, especially <.com> domain names, are highly valued in today's marketplace. For example, this past year, <sex.com> sold for \$12 million, <diamond.com> purportedly commanded \$7.5 million, and <vodka.com> was purchased in the \$3 million range. *Vodka.Com Domain Sells For \$3 Million*, DOMAINNEWS.COM (Dec. 16, 2006), at <http://www.domainnews.com/aftermarket/0920061216/vodkacom-domain-sells-for-3-million/> (last visited July 2, 2007). Because of the value attributed to domain names, cybersquatting and other illegal and unfair uses of trademarks on the web remain a source of major concern.

Cybersquatting is nothing new, but certainly deserves the continued attention of brand owners and their counsel. Cybersquatters are buyers of domain names that incorporate another's trademark, with a bad-faith attempt to profit from holding those domain names. According to a recent study of some of the world's strongest brands by a leading trademark monitoring service, cybersquatting increased nearly three-fold during 2006 alone, and by another thirty-three percent in 2007. *MarkMonitor, Brandjacking Index* (Apr. 30, 2007); *MarkMonitor, Brandjacking Index* (Winter 2007). This increase is due, in part, to the new trends in the domain name infringement arena discussed below.

Domain name tasting. A five-day grace period exists, during which a domain name registration may be rescinded, without the buyer (known as a registrant) incurring the usual registration fee. The listed purpose for this policy is to remedy typographical errors and the like that can occur during the registration process. However, some unscrupulous companies are using this grace period to test the marketability of certain domain names, many which consist of misspellings of company and brand names. The registrants track the amount of traffic received at those sites, and cancel the lesser visited domain names with no fee or penalty. Approximately four million domain names are tasted each day, and this practice is only increasing. *National Arbitration Forum, Critics grow as "Domain Tasting" Becomes More Prevalent* (Jan. 24, 2007), at <http://www.adrforum.com/rcontrol/document/newsletters/DomainNews-Vol08No01.htm> (last visited May 24, 2008) (noting comment of Jay Westerdal of Name Intelligence).

Domain name kiting. Some "domain name tasters" register domain names, drop them within the five-day grace period, then reregister them, and continue this approach in perpetual cycles. This activity, referred to as domain name kiting, provides domain name owners with an economic bene-

fit, as they receive money when visitors to their websites click on advertising links therein. Not only do these sites crowd the Internet, but they also may cause various harms to brand name owners, including customer confusion, loss of goodwill, and loss of revenues.

Domain name spying. This development involves the practice of purchasing domains shortly after learning that an interested party checked their availability. Put another way, the companies that perform this activity monitor third parties' searches for domain names that may contain new trademarks, and then purchase domain names containing those phrases before the rightful owners can obtain them. Some companies appear to make spying their entire business model; thus, this practice might not be as rare as you might expect.

Phishing. Some thieves operate by sending out emails to divert people to websites that appear very similar to companies' true sites, but are instead phony sites used to obtain personal financial information. Banks and other companies in the financial sector are the most common targets of phishing schemes. In addition to stealing money and identifications, phishing has been dissuading many people from transacting business online, and it could lead to less business for some companies.

What Can You Do to Protect Your Client's Brands From Such Attacks on the Internet?

Several steps may be taken to prevent cybersquatting, including:

- **Registering key domain names.** A company can never own all possible domain names that incorporate its brands. However, companies should consider purchasing the obvious spellings and misspellings of its primary brands, with the extensions that are most commonly used and searched, namely .com, .net, and .org. If the company conducts business outside of the U.S., or is likely to do so in the near future, then also consider registering domain names with the appropriate "country code" extensions, such as .ca (for Canada), .cn (for China), .co.uk (for the United Kingdom), or .eu (for Europe). Use experienced intellectual property counsel to obtain Chinese domain names and keywords. The best offense is defensive registration.
- **Registering without hesitation.** To avoid domain name spying, companies should register domain names of interest as soon as they learn that the domain names are available, and use only reputable companies

continued on page 9



Protecting Your Client's Brand... *continued from page 8*

to conduct searches.

- **Renewing domain names.** Remember to prompt your client to renew the domain names it has acquired. Some companies configure their domain name settings to automatically renew the domains annually, or purchase them for years in advance to minimize the need for monitoring them. Also, make sure that any departing employee hands over access to company domain names.
- **Monitoring the Internet.** Several services charge annual fees to monitor the Internet for possible infringement of key brands, and intellectual property counsel can assist with this process. There are also free websites that companies can use for searching for domain names incorporating your trademarks or company names, such as Namedroppers.com and Tldscan.com.

What Can You Do If a Third Party Has Already Registered a Domain Name that Is Valuable to Your Company's Business?

Various enforcement tactics could be considered, including the following:

- **Sending a demand letter.** Sending a cease and desist letter is a common, simple and cost effective method to acquire a domain name.
- **Offering to purchase the domain.** Consider making an anonymous offer to the registrant to buy the domain name at issue. Concealing the company's identity could improve the likelihood that the registrant will agree to sell for a reasonable amount.
- **Placing a backorder for the domain name.** Another tactic is to consider placing a backorder to purchase the domain name, whereby the company can get in line to offer to purchase it. Typically, backordering services only charge a fee (and a relatively small one, at that) when the backorder is successful.
- **Filing an administrative complaint.** A procedure governed by the Uniform Domain Name Dispute Resolution Policy (UDRP) allows for the filing of an administrative complaint to request that a domain name be transferred. This procedure is available in many instances of cybersquatting and, depending on the company's goals, can be more cost-effective than proceeding with litigation. The most popular service providers for this procedure are The World Intellectual Property Organization ("WIPO") and The National Arbitration Forum ("NAF").
- **Filing a lawsuit.** In some instances, the facts might warrant proceeding with litigation. For example, a California court recently enjoined a company from registering any domain names confusingly similar to

Verizon's trademarks, after the court reviewed the defendant's domain name tasting, kiting, and other cybersquatting activities. *Verizon Cal. Inc. v. Ultra RPM, Inc.*, No. 2:07-cv-02587-PA-CW (C.D. Cal. Sep. 10, 2007). Dell is also suing a handful of registrars for a variety of allegedly abusive domain name registration practices. *Dell Inc. v. Belgiumdomains, LLC*, No. 07-22674 (S.D. Fla. Oct. 10, 2007). Additionally, note that, under certain laws, significant monetary damages may be awarded. For instance, under the Anti-Cybersquatting Consumer Protection Act of 1999, a company could be entitled not only to transfer of the domains at issue, but also treble damages, attorneys' fees, and statutory damages of up to \$100,000 per domain name. 15 U.S.C. §1125(d).

Conclusion

Companies are unlikely to prevent or stop all unfair and illegal activity on the Internet affecting their trademarks. Additionally, the vast size of the Internet and large scale of cybersquatting can be overwhelming. However, taking some of the steps listed above can be extremely useful in protecting valuable brands.

As with all areas of the law, the most appropriate steps to take will vary depending on each scenario. Factors to consider include the importance of the domain name and brand to your client's business, your client's budgetary constraints, the timeframe by which your client desires to retrieve the domain name, the type of website content currently found at the domain name of interest, and the history and current behavior of the domain name registrant.



* *Debra Y. Hughes is Assistant General Counsel for Wal-Mart Stores, Inc. In her current position, Ms. Hughes manages the company's domain name portfolio, counsels business clients regarding a wide array of trademark, patent, copyright and publicity concerns, and manages the design and packaging review process for Wal-Mart's private label products. She also is a member of the Internet Committee for the International Trademark Association.*



David A. Bell is an Associate in the Dallas office of Haynes and Boone where he concentrates his practice on trademark law. Mr. Bell manages clients' comprehensive brand portfolios and prosecutes their trademarks before the United States Patent and Trademark Office. He also has unique experience helping his clients defend their trademarks on the Internet by addressing legal issues such as domain name abuse and keyword advertising.