Battling Cyberpirates

***Franchising World*, August 2005**

While it is not possible to prevent all cyberpiracy, it can be drastically curbed by monitoring trade name and mark use on the Internet, and pursuing appropriate actions against cyberpirates.

By Lee J. Plave and Inna Tsimerman

Clashes over domain names are becoming more common as the number of domain names proliferate and cyberpirates become more audacious. Cybersquatters register as domain names the trademarks and trade names of businesses and even the names of famous people with which they have no connection. They profit from the first-come, first-served nature of the domain name registration system, and use these businesses' and individuals' good names to attract users to their own Web sites. Cybergripers incorporate the trademarks, trade names or individual names of businesses or famous people with which they have no connection in domain names, then use the domain names in connection with Web sites critical of the businesses' or individuals' products, services, beliefs or business practices.

So what happens if you become the victim of a cyberpirate? Here are some mechanisms that you can use to identify cyberpirates and then describes the remedies available against them.

Catching Cyberpirates

Franchises should monitor the Internet for cybersquatters and cybergripers even before problems arise by assigning the task to employees, or traditional trademark or more specialized Internet watching companies. You should also encourage employees, customers, vendors and the like to watch for unauthorized use of your trademarks and domain names identical or confusingly similar to your name or trademarks.

Discovering the Identity of Cyberpirates

"WHOIS"

The Internet Corporation for Assigned Names and Numbers, which has responsibility for generic and country code Top-Level Domain name system management, maintains a database which allows users to search for the registrars of domain names in the.com, .edu, .net, .org and other service TLDs. UWHOIS, Inc. maintains a similar database for domain names in most country code TLDs.

Additional information regarding domain name registrations can be gleaned from the registrar's Web site. A list of ICANN-accredited registrars can be found at www.internic.net/. Generally, the contact information (name, address, e-mail and phone number) provided by domain name registrants is available in a public whois database. For example, the whois database of Network Solutions, Inc. is the largest registrar of gTLD domain names. However, NSI and some others registrars have established "private" registration programs under which registrants' contact information can be kept outof the public whois database.

Registrants are required to provide accurate and updated registrant and contact information under the terms of registration agreements which they must enter into before registering any domain name. However, it is easy to provide false information because few registrars verify such information and, even if originally accurate, registrants can change this information at any time.

Investigators and Other Self-Help Tools

If domain names resolve to active Web sites, information regarding registrants may sometimes be gleaned from the Web sites' contents. Some cyberpirates may have provided identifying information when they originally posted their Web sites but have since then removed. Some resources, such as the Internet Archive Wayback Machine service allow users to view Web sites as they appeared in the past. Unfortunately, no resource archives all Web sites, and operators can take measures to prevent their websites from being crawled.

Lawyers and private investigators who know how to track domain trademark infringers and counterfeiters can also be helpful in gathering

information.

Subpoenas

The most effective way to get information about cyberpirates is often to issue a subpoena to the relevant registrar for all information and records related to domain name registration, renewal and maintenance. Responses typically generate information originally provided by the registrant to pay for the domain name (for example, credit card information). Subpoenas can also be submitted to credit card issuers. Note that it can be difficult to compel registrars located outside the United States, Canada and the European Union to comply with subpoenas or other requests for information.

However, subpoenas can only be issued by courts in which actions concerning the subject matter of the subpoenas is pending. Below we discuss how a court action against a domain name registrant can be commenced in the United States.

Domain Name Transfers and Other Relief

The two main means of recourse against cyberpirates are arbitration under ICANN's Uniform Domain Name Dispute Resolution Procedure or litigation. In the United States, trademark owners can seek remedies in the courts, chiefly pursuant to the federal Anticybersquatting Consumer Protection Act of 1999. Once a registrar receives notice of a UDRP action or a court or arbitral action, the registrar will "freeze" the domain name, prohibiting any transfers or changes to the whois information by the registrant. Both the UDRP and ACPA permit trademark holders to pursue recourse against cyberpirates without knowing their true identity, and in both the use of false registrant information will serve as evidence—which, however, is refutable—of the registrant's bad faith.

UDRP

As part of domain name registration agreements, all ICANN-accredited registrars require registrants to submit to administrative proceedings if initiated under the UDRP.

Remedies Available: The only remedies available under the UDRP are cancellationor transfer to the complainant of the domain name registration.

Proof Required/Criteria: To succeed in a UDRP proceeding, the complainant must show that the registrant has registered a domain name that is identical or confusingly similar to a trademark or service mark in which the complainant has rights; no rights or legitimate interests in the domain name; and registered and is using the domain name in bad faith.

A registrant can demonstrate its rights or legitimate interests if the registrant used the domain name in connection with a *bona fide* offering of goods or services; has been commonly known by the domain name; or is making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark at issue.

Bad faith can be shown by many means, including indications that the registrant has acquired the domain name to sell, rent or otherwise transfer it to the owner of the trademark or to the owner's competitor for valuable consideration in excess of the registrant's costs; the registration of the domain name to prevent the trademark owner from reflecting the mark in a corresponding domain name, where there is a pattern of such conduct; the registration of the domain name primarily to disrupt a competitor's business; or use of the domain name to attract, for commercial gain, Internet users to the registrant's Web site by creating a likelihood of confusion with the complainant's mark.

The ACPA and Other Legal Remedies Under U.S. Law

The ACPA is a powerful tool for trademark holders.

Remedies Available—ACPA: In a successful ACPA lawsuit, plaintiffs are awarded transfer of the domain name and damages, including statutory damages that range from $1,000 to $100,000 per domain name, and legal fees. ACPA also provides for *in rem* jurisdiction, where the domain name registrant cannot be located is not subject to the *in personam* (personal) jurisdiction of U.S. courts (e.g., where the registrant is outside the U.S. and does not conduct business in the U.S.). In *in rem* actions, as in actions under the UDRP, the courts cannot assess money damages.

Proof Required/Criteria: In order to succeed in an ACPA claim, the plaintiff must show that the domain name registrant has a bad faith intent to profit from the plaintiff trademark holder's mark; and registered, traffics in or uses a domain name that, in the case of a mark that is distinctive at the time of domain name registration, is identical or confusingly similar to the plaintiff's mark, or, in the case of a famous mark that is famous at the time of domain name registration, is identical or confusingly similar to or dilutive of the plaintiff's mark.

Courts will consider the following factors (among others) in determining bad faith intent:

- the registrant's trademark or other rights in the domain name;
- the extent to which the domain name consists of the registrant's name;
- the registrant's prior use of the domain name in connection with the *bona fide* offering of any goods or services, and noncommercial or fair use of the mark in a site accessible under the domain name;
- the registrant's intent to divert consumers from the trademark owner's Web site, either for commercial gain or to tarnish or disparage the trademark owner's mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the domain name registrant's Web site; and
- the registrant's offer to transfer, sell or otherwise assign the domain name to the trademark owner or any third party for financial gain.

Other Causes of Action: For a domain name that is identical or similar to a plaintiff's trademarks, bad faith may also provide the basis a claim of trademark infringement, unfair competition and trademark dilution actions under U.S. law. In addition, depending on what materials, products or services are advertised or made available on a Web site to which the domain name at issue resolves, there may be a cause of action for copyright infringement, trade secret misappropriation, or defamation. A successful plaintiff in these cases may also be awarded statutory damages and attorneys fees.

Comparison—Advantages and Disadvantages

When battling a cyberpirate, the best course of action depends heavily on the circumstances of the case, the party whose name is being pirated, and the strength of the mark at the heart of the case.

Time and Money:A UDRP action may be the more economical, and streamlined option.

UDRP disputes are supposed be resolved within 45 days of the initial filing, without in-person hearings or cross-examinations. U.S. federal courts actions, especially contested actions, can often take months or longer to resolve.

For proceedings involving 1 to 5 domain names, the World Intellectual Property Organization, the most popular ICANN-approved domain name dispute resolution provider, charges panel filing fees of: $1,500 for a single panelist, $4,000 for three panelists.

While U.S. court filing fees are generally lower, the costs of litigation can run high in contested actions. There is a possibility, also, that the defendant will counterclaim, raise defenses (e.g., the validity of the underlying trademark registration), and try to take discovery against the plaintiff trademark owner.

Possibility of Damages and Injunctive Orders: Most importantly, the ACPA allows for damage awards to successful plaintiffs (except in *in rem* actions), and permits plaintiffs to seek immediate injunctions to shut down cyberpirates' Web sites. Also, plaintiffs may seek judgment orders not only for transfer of the domain names, but also to require domain name registrants to stop and abstain from registering or using any domain names, marks or trade names which are identical or confusing similar to that of the plaintiffs. If registrants violate the order, plaintiff trademark holders may be able to pursue a contempt action as well for violation of the order.

Implementation of Decisions by Registrars: All ICANN-accredited registrars are required to implement decisions of UDRP panels without additional action. While registrars will generally transfer or cancel domain name pursuant to a court order, registrars established outside the U.S. may require a plaintiff in an ACPA action to obtain an enforcement order from a local court in the country where the registrar is established prior to implementing the decision, resulting in additional and significant expenses.

Finality of Decision: While ACPA and other actions in U.S. courts can be appealed, the costs of such appeals may be prohibitive. However, either party may institute an arbitral or court action during or following a UDRP action. Registrars will even wait 10 business days before implementing a UDRP decision to transfer or cancel a domain name registration in case a judicial proceeding regarding the domain name is instituted.

Lee Plave (lee.plave@dlapiper.com) is a partner and Inna Tsimerman (inna.tsimerman@dlapiper.com) practices law with DLA Piper Rudnick Gray LLP in the firm's Washington, D.C. and Chicago offices, respectively.

Find this article at:
http://www.franchise.org/Franchise-News-Detail.aspx?id=40580

☐ Check the box to include the list of links referenced in the article.