A Solution for Businesses Victimized By Internet Identity Theft.

It's a business nightmare. The Acme Loan Corporation has a website, www.acmeloan.com, which potential borrowers visit to apply for home, auto and personal loans. Unbeknownst to Acme Loan, however, scam artists obtain a very similar domain name, www.acmeloan.*net*, and set up a website nearly identical to Acme's legitimate website, complete with Acme Loan's registered trademarks. When consumers are directed to the scammers' site by search engines or email solicitations and apply for loans, the scammers advise consumers that their loan applications have been approved, and will be funded upon receipt of an $800 "application fee" from the consumer. The $800 is paid, the loan never funds, and the angry consumers then call your client, the real Acme Loan Corp., demanding their loans or their money back. The goodwill associated with Acme Loan's trademarks begins to take a heavy hit.

Of course, when Acme's lawyers contact the domain registrar controlling the .net domain to find out who is operating the offending website, they learn that the scam artists have given the domain registrar phony addresses and contact information. What can Acme Loan do to prevent further damage to its reputation, and further losses to consumers?

One fast and effective remedy is provided by the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (hereinafter "the Act"). Enacted in 1999 by Congress as an amendment to the Lanham Act, which generally protects trademarks, subsection (d)(1)(A) imposes civil liability in favor of a trademark owner against any person who: i) has a bad faith intent to profit from that trademark; and ii) registers, traffics in or uses a domain name that in the case of a trademark that is distinctive at the time of registration of the domain name and is identical or confusingly similar to that trademark. The Act sets forth the factors the Court may consider in deciding whether a person has the required "bad faith intent" to profit from a protected trademark.

Frequently, however, the "person" responsible for the mischief can't be found or, for obvious reasons, has given misleading information in registering the domain name. Who do you sue? 15 U.S.C. Section 1125(d)(2) again provides a solution: "The owner of a mark may file an *in rem* action against a domain name in the judicial district in which the domain name registrar domain name registry or other domain name authority that registered or assigned the domain name is located * * *."[1] In other words, an action may be filed against the misappropriated domain name itself instead of against an individual or corporate defendant. Such an *in rem* action may be filed if (i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office or is otherwise protected by the Lanham Act, and (ii) the court finds that the owner of the mark is not able to obtain in personam jurisdiction over a person who would have been a defendant in the civil action created by the Act, or that the owner through due diligence has been unable to find a person who would have been a defendant.

[1] ***In rem*** is Latin for "in a thing". In a lawsuit, an action *in rem* is directed towards some specific piece of property, rather than being a claim for, say, monetary compensation against a person (which is an *in personam* or personal action). It focuses on proprietary title to property. Land is an example of a case where, when the title (e.g. who owns a house) is in dispute, an *in rem* action is used to deliver the land itself back to the rightful owner. An *in rem* action thus makes the property itself the nominal defendant. See http://en.wikipedia.org/wiki/In_rem.

What due diligence does the owner of the trademark have to use before filing an *in rem* action? The Act specifies that the owner must send a notice of the alleged violation and intent to proceed *in rem* to the registrant of the domain name at the postal and e-mail address provided by the registrant to the domain name registrar, and must publish such notice of the action as the court may direct promptly after filing the action. The good news is that if the owner of the mark complies with the notice prescribed by the Act, the notice itself constitutes service of process. 15 U.S.C. § 1125(d)(2)(B).

Once the *in rem* action is filed and is deemed to have been served on the domain name, the owner of the mark simply needs to send written notification of a file-stamped copy of the Complaint to the domain name registrar. Upon receipt of the file-stamped Complaint the Act requires the domain name registrar to deposit expeditiously with the Court documents sufficient to establish the Court's control and authority over the domain name during the pendency of the action. In addition, the Act precludes the domain registrar from transferring, suspending, or otherwise modifying the domain name during the pendency of the action except upon order of the Court.

Although the only available remedy in such an *in rem* action is a court order for the forfeiture or cancellation of the domain name, or transfer of the domain name to the owner of the mark, the Act makes it clear that this remedy is not exclusive: should the owner of the mark locate the offending prior registrant of the domain name, a civil action would still be possible despite the *in rem* proceeding.

So what should Acme and its lawyers do upon learning that cyber pirates have set up using Acme's trademarks and a confusingly similar domain name? They can take a page from the playbook used by Dillingham & Murphy lawyers J. Cross Creason and Bill Murphy recently to help a New York City law firm and its client.

1. **Identify the domain name registrar for the domain name, as well as who registered the domain name, and the mailing and email addresses of the registrant.**

Use a web-based WHOIS[2] query tool to obtain the WHOIS data for the domain name, including the name of the domain name registrar, as well as the name, postal address, and email address of the registrant of the domain name.

2. **Send notice of intent to proceed *in rem* to the registrant.**

Send a notice of the alleged violation of the owner's trademark rights, and intent to

[2] "WHOIS services provide public access to data on registered domain names, which currently includes contact information for Registered Name Holders. The extent of registration data collected at the time of registration of a domain name, and the ways such data can be accessed, are specified in agreements established by ICANN for domain names registered in generic top-level domains (gTLDs). For example, ICANN requires accredited registrars to collect and provide free public access to the name of the registered domain name and its nameservers and registrar, the date the domain was created and when its registration expires, and the contact information for the Registered Name Holder, the technical contact, and the administrative contact" (see http://www.icann.org/en/ topics/whois-services/)

proceed *in rem* against the offending domain name under 15 U.S.C. Section 1125(d)(2), to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar (15 U.S.C. § 1125(d)(2)(A)(ii)(II)(aa)).

3. File the Complaint.

The Complaint is properly filed for jurisdiction and venue purposes in the federal judicial district in which the domain name has its situs, defined as the judicial district in which "(i) the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located; or (ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the Court" (15 U.S.C. § 1125(d)(2)(C)).

4. Deliver a copy of the Complaint to the registrar; give notice to the cyber pirate.

After filing the Complaint, the next step is to deliver a copy of the Complaint, file-stamped by the district court to the domain name registrar. Upon receipt of a file-stamped copy of the Complaint, the domain name registrar is required by 15 U.S.C. Section 1125(d)(2)(D)(i) to deposit with the district court documents sufficient to establish the court's authority regarding the disposition of the registration and use of the domain name. Additionally upon receipt of the file-stamped copy of the Complaint, the domain name registrar is prohibited from transferring, suspending, or otherwise modifying the domain name during the pendency of the action, except upon order of the court. Although domain name registrars should be aware of their obligations under 15 U.S.C. Section 1125(d)(2)(D)(i), it is advisable to remind the registrar of those obligations upon delivery of the Complaint.

The court may also direct the owner of the mark to publish notice of the action. Service of process is achieved by means of the pre-Complaint notice to the cyber pirate set out above (Step #2) in addition to any post-Complaint publication required by the court (15 U.S.C. § 1125(d)(2)(B)).

5. Prevent continuing misuse of the domain name during the pendency of the action.

In order to prevent ongoing harm caused by the misuse of the domain name after the Complaint has been filed, the owner of the mark may wish to seek an early temporary restraining order (TRO) and preliminary injunction ordering the domain name registrar to temporarily transfer the domain name to the owner of the mark pending final judgment in the *in rem* action. A temporary restraining order for the transfer of a domain name in an *in rem* action is appropriate where the use of the domain name may cause irreparable harm. *Broadbridge Media, L.L.C. v. HyperCD.com, an Internet Domain Name*, 106 F. Supp. 2d 505 (S.D.N.Y. 2000), although the Courts have not uniformly agreed.

As an alternative interim remedy, the owner of the mark may seek a TRO and preliminary injunction ordering the domain name registrar to disable the domain name pending final judgment. In either event, the Court will insist on security as a condition of the entry of a temporary restraining order and/or a preliminary injunction. Be prepared to have the client cut a check for security promptly.

6. Take the Defendant's Default and Secure Entry of A Default Judgment

After the time for the Defendant or other interested persons to respond has expired, the Plaintiff may file a notice of default with the Court. However, taking the default of the defendant is not the same thing as having a default judgment entered. Simply because the defendant has not appeared, don't assume that the Court will enter default judgment at the Plaintiff's request, and without a requisite showing.

You should, for example, comply with Rule 55(d) of the Federal Rules of Civil Procedure. You must establish that the defendant is not a minor or an incompetent person, and that the defendant does not have military status. FRCP 55(b)(2); 50 U.S.C. App. § 521.

The decision to grant or deny an application for entry of default judgment is a matter within the Court's discretion. The factors a court may consider in determining whether a default judgment should be entered include: (a) the merits of plaintiff's substantive claim and the sufficiency of the complaint; (b) the possibility of prejudice to the plaintiff; (c) the sum of money at issue in the action; (d) the possibility of a dispute concerning material facts; and, (e) whether the default was due to excusable neglect. *Eitel v. McCool*, 782 F.2d 1470, 1471-1472 (9th Cir.1986). Each of these factors should be discussed in a brief supported by evidence accompanying the application for entry of default judgment. Failure to adequately support the application may result in its denial. *CNF Inc. v. THECNF.COM* 2006 WL 3388577 (N.D.Cal.2006) [service of complaint on Domain Name Registrar was not adequate service of process to support default judgment where plaintiff had actual knowledge of name and address of entity which registered THECNF.COM]; *Corair Memory, Inc. v. CORSAIR7.com* 2008 WL 4820789 (N.D.Cal.2008) [in denying application for default judgment, court weighed several factors, including all nine factors set forth in the Act for evaluating "bad faith attempt to profit" from allegedly misappropriated domain name, the availability of an alternate remedy under ICANN's Uniform Domain Name Dispute Resolution Policy, the apparent failure of plaintiff to publish notice as directed by the court under § 1125(d)(2)(A)(II)(aa)-(bb), and unavailability of relief sought in that domain name's registration had expired as of time of application].

7. Transfer of the Domain Name to Plaintiff.

Next, prepare for an eventual default judgment ordering the domain name be transferred to your client by setting up an account for your client with the domain name registry or registrar with which the offending domain name is currently registered, or with a new domain name register or registry. This account creates a destination to which the current domain name registry or registrar can transfer the name once presented with the court's order. Setting up an account is fairly simple and, depending on the domain name registry or registrar, can be accomplished through an on-line application. As a practical matter, setting up an account for your client with the current domain name registry or registrar may expedite the transfer to your client's control. Once the domain name is transferred an account controlled by your client, a decision can then be made to transfer the domain name to another domain name registrar or registry or leave it registered with the current domain name registrar or registry.

Conclusion.

By leveling the playing field on which the trademark owner pursues the remote cyber pirate, the Anti-Cybersquatting Consumer Protection Act provides both and expeditious and appropriate method of establishing jurisdiction and a fast remedy for on-line trademark infringement.