PROFESSIONAL POINTERS

Don't Be Fooled By These Brand Protection Scams

Mike Serra
Senior Associate at Bodman PLC, Michigan State University Alumnus, B.A. Political Science

Scams seem to overrun the internet. Most scams, like selling counterfeit goods or phishing (fake emails used to obtain private information), try to confuse your customers. This makes sense. Why would an internet outlaw pick a fight with ***you***, the seasoned brand protection professional? Yet even the most sophisticated sometimes get fooled by internet scams. Below are a few brand protection scams that are directed at brand owners rather than their customers.

Fraudulent Trademark Invoices. Every good brand owner knows the value of a trademark registration. Fraudulent invoice scams prey on brand owners' instincts to promote protection of a brand as a way to score an easy buck. Like Judo, scammers see your enthusiasm and then leave you on your back.

Scammers send legitimate looking invoices requesting fees to complete a trademark registration. These invoices are particularly confusing because scammers use actual trademark filings to find familiar names, marks, serial numbers, and other indicia of legitimacy. To make matters worse, invoices come from legitimate sounding entities. The U.S. Patent and Trademark Office (USPTO) has identified some of these fraudulent entities as "Patent & Trademark Resource Center," "Patent and Trademark Organization," "U.S. Trademark Compliance Office," and "Patent & Trademark Office." You can see the USPTO's full list of such entities at USPTO. At the bottom of this article is just one example of a fraudulent invoice from the "Patent & Trademark Resource Center."

> **Takeaway.** You must learn to spot a fake when you see one. If you come across what you think is a fraudulent trademark invoice, check with your trademark agent in the region, trusted outside brand protection counsel, or your internal trademark staff, to determine if it is legitimate. You can also cross-reference the invoices with the USPTO list of known scammers. But what happens if you mistakenly pay a scam invoice? You can talk to a lawyer; recovery may be an option through a civil suit [LINK See BPP 2nd Edition "Leveraging Consumer Feedback to Identify and Combat Counterfeiting"]. Keep in mind that issues with jurisdiction may flow from legal actions of that sort and cost may outweigh recovery.

The Domain Registry Scam. This scam involves an email from an alleged domain registry "warning" you that some third-party is attempting to register domain names using your trademarks. Scammers find important marks and contact information by mining your trademark portfolio or legitimate domain names. They then list numerous domain names that are allegedly being registered and ask for your "permission" to allow registration. Once you reply, "no no no, that's ***my*** name," the scammer sends you a contract with inflated prices and extended terms to "register" those domains before "someone else" does.

> **Takeaway.** Scammers are targeting your brand protection instincts. It is natural to react aggressively when you hear about someone trying to steal your goodwill. That "good Samaritan" informing you of the potential registration, unfortunately, is only trying to take your money, so learn to recognize such emails and ignore them.

"Potential Opposition" Emails. This scam is similar to the domain registry scam. Although some may see it as a legitimate attempt to drum-up business, it is, at the very least, deceptive advertising. It works by sending emails with bold letters stating "potential opposition" to those filing foreign trademark applications. What's wrong is that such emails are written to confuse brand owners into believing that their applications are subject to a foreign opposition proceeding when they are not. Brand owners think they have a duty to respond as if there was an "opposition" pending, when really the email is only notifying recipients of potentially conflicting foreign marks. Below is a redacted header of a scam email that was recently sent to me:

> Re: Potential oppositions against the marks "[redacted]" in China (Your Ref.:
> Please advise; Our Ref.: [redacted])
> Client: The [redacted]
> **Deadline to Oppose: July 6, 2017, Beijing time, NOT extendable**

Takeaway. The point here is that brand owners must understand that emails like this are not mandating any action in the foreign jurisdiction. They are just a form of international "marketing".

Negotiating with a Cybersquatter. Cybersquatting has been written about at length (see BPP 3rd Edition on ICANN's gTLDs and BPP 4th Edition Cover Story on cyber crime). It is generally defined as the practice of registering domain names for well-known brands in an attempt to sell those domains for profit. The part of this scam you should avoid is actually negotiating with cybersquatters. There are alternatives other than resorting to extortionist prices. Namely, you may file a Uniform Dispute Resolution Policy ("UDRP") complaint, a lawsuit through the Anticybersquatting Consumer Protection Act, or if there are counterfeits being sold on the domain, a lawsuit under the Lanham Act. These options, though, could get relatively expensive if you need to hire an outside attorney. UDRP complaints have also been criticized for being slow and inefficient where there is widespread cybersquatting.

Takeaway. Brand owners can get caught up in games with cybersquatters. You must assess the value of the subject domain and what is shown on the website before even approaching a cybersquatter. The better value might be building your web presence from a variation of your mark or by using a different top-level domain (for example, ".us," ".biz," or ".net"). On the other hand, the cost of a UDRP complaint or lawsuit may be worth it if your brand is particularly well-known or the cybersquatter begins using its domain to confuse customers, sell counterfeits, or otherwise tarnish your reputation.

The point is to make sure you stay vigilant. You might not run into the scams identified above, but you should be wary of those trying to make a buck off of your efforts to protect the brand. Indeed, you do not want to be the subject of my next article on this issue.