Podcast Transcript

Trademark and Copyright: The Good Fight

Date: May 16, 2024

Guest: Kevin Bovard, **Host:** Leeann Lee

Run Time: 10:20

For questions and comments contact:

Kevin Bovard

Partner
Philadelphia
T: +1.215.564.2727 | kbovard@bakerlaw.com

Lee: Clients have increasingly been on the receiving end of false and misleading trademark related scams. Scammers have become more sophisticated and are targeting brand owners in multiple ways. Targeting both would-be trademark applicants and established registrants. I'm Leeann Lee and you're listening to BakerHosts.

On today's episode, we discuss web domain scams and the uniform domain name dispute resolution policy. We'll also discuss a recent wave of spam solicitations for trademark prosecution services. To provide us with insight into this topic, we have Kevin Bovard, a partner in the Intellectual Property Group at BakerHostetler. Kevin is a member of the Trademark and Copyright team and is an accomplished intellectual property practitioner with a focus on copyright and trademark matters. His areas of concentration include trademark clearance, worldwide portfolio management, copyright protection, unfair competition, domain name disputes, IP due diligence and litigation in federal court and before the Trademark Trial and Appeal Board. Welcome to the show, Kevin.

Bovard: Hi Leeann. Great to be here.

Lee: So, to start out, I know you've dealt with increasing numbers of fake websites that pose as brand owners. Tell us what you've seen lately.

Bovard: That is exactly right, Leeann. The brand owners have been facing this problem for a number of years, but the numbers have been only going up. We're seeing increasing numbers of websites set up posing as the actual brand owner. Sometimes these are used just for the e-mail addresses and those e-mail addresses may be used in phishing scams. Other times, we're seeing websites being set up that look exactly like the brand owner's website. They might use the brand owner's trademark, logo, and even crib the text of the brand owner's website to make it all look and feel very much like a real, true website. Particularly in nefarious instances, the bad actor will include a login page which they're presumably using to scrape the customer's login and password information. So, to combat this, many brand owners are employing domain monitoring services. They can either do that themselves or we can do it on our end and these services will monitor for newly registered domains that are similar to the brand owners. We can then evaluate them to see what type of content is coming up on the domain and evaluate whether there is anything else that may be suspicious about the domain registration. This often allows us to catch the bad actors and get a head start before they actually perpetrate any kind of serious fraud.

Lee: Okay. So, are there any industries that are being particularly hard hit?

Bovard: Virtually, all industries where something is being sold are being hit. The statistics show that banking and finance is being particularly hard hit. Over 11 percent, I believe this past year's fraudulent complaints were in the banking and finance industry. But any sort of brand owner could be targeted, whether you're in pharmaceuticals, in medical devices, retail, clothing and fashion. If you're selling something, if money is involved in transactions of your business, there is a possibility that a bad actor could be targeting you.

Lee: So, with that in mind, what types of legal action are you taking to mitigate these fraudulent schemes?

Bovard: So, the most aggressive course of action that a client or a brand owner could take would be to file a District Court litigation. These bad actors are typically anonymous. The issue is that you're going to have to file this as a John Doe lawsuit, and the reality is these bad actors are very likely using VPNs and other tools to keep their identity virtually impossible to ascertain. So, District Court litigation is very improbable in terms of likelihood getting meaningful success at a reasonable price. So, what we do instead, most frequently, are to file either a DMCA complaints or UDRP complaints. DMCA stands for Digital Millennium Copyright Act, and if the bad actor has borrowed or stolen the brand owner's logo or the text of their website, those are possibly subject of copyright, and in that case we can submit a DMCA complaint, a takedown demand, to the web host that is hosting the domain.

If the bad actor has used a web host that is outside of the United States, the web host would not necessarily be subject and likely isn't subject to the DMCA, the Digital Millennium Copyright Act. Instead, we would utilize our colleagues in whatever foreign jurisdiction the web host is located in and have them assist us with whatever comparable takedown strategy is available in that country. The other option is to file what is called a Uniform Domain Dispute Resolution Policy or UDRP complaint. This is when the bad actor has registered a domain that incorporates the brand owner's trademark in the URL or something closely approximating the client owned trademark in the URL. In this case, even if there is no content up on the website yet, for instance, the scenario where the bad actor is simply using e-mail addresses from that URL, we are able to file the UDRP complaint. It is a fairly quick and easy process where we file the complaint, the bad actor in theory has an opportunity to respond, although they virtually never do, and then a decision is quickly rendered by the panelist who is appointed to make the determination of the UDRP complaint. Then once we receive a favorable decision, within 10 days of a decision, the registrar is required to transfer the domain to the brand owner's control. They can then repurpose the website. They can shut it down, or simply redirect it to their actual legitimate website.

Lee: So, I also understand that clients have been receiving scam solicitations for trademark services. What is going on there?

Bovard: Well, Leeann, as our listeners likely know, the PTO's records are all public. So, for a number of years now, we've been seeing bad actors writing to trademark registrants, perhaps up to two years ahead of trademark renewal deadlines and they'll send what looks to be an invoice, an official looking document, to the brand owner and they say, return this with your payment of $2,000 and renew this trademark. They often use names that are very official sounding like World Trademark Register or Trademark Registration Office, but these are all fake. They have nothing to do with the USPTO. More recently, we've been seeing phone calls where the bad actors will spoof the phone line to appear to be calling from the USPTO then they say that fees are due. In fact, this isn't the USPTO, it is a bad guy on the line. The USPTO will never call the registrant seeking fees. More recently, we've been seeing outfits targeting companies that don't have registrations. Here, the scammer reports to be an attorney and they say we have a client seeking to register your brand name. Let us know if this is a problem and we'll help you register the mark. Obviously, the brand owner doesn't want a third party to register the trademark, so they may be susceptible to responding. But in fact, they shouldn't. They should reach out to a real trademark attorney who they know and who they can trust if they actually do want to pursue a trademark application.

Lee: Well, with that in mind, is there anything that our clients can do when they receive these scams and what should they be looking out for?

Bovard: Well, they should review any contact from an unknown party with a careful eye and some suspicion. If you used an attorney to file a trademark application, all communications from the PTO are directed to the attorney of record. And all PTO correspondence is electronic now. So, if you receive something in the mail, it is very likely not legitimate. Same if you receive a phone call, not likely to be legitimate. At the end of the day, brand owners simply have to be vigilant and be on the lookout for something that might be suspicious.

Lee: Well, I have one last question for you. What does the future portend with these bad actors and is any help on the horizon?

Bovard: Well, unfortunately, I'm afraid that we can only expect these bad actors to get more creative in their attempts to defer money and otherwise scam brand owners. No fail safe tools appear to be on the horizon, but one new option may be available to some of our larger brand owners. The U.S. Department of Homeland Security has recently begun offering what they call vulnerability scanning for major companies web portfolios. Now, the hitch here is you have to be what is called a quote, private sector critical infrastructure organization. This would be brand owner like a bank, a utility company, maybe a social media company. If the brand owner thinks they fall into this category, they may want to explore this option. Otherwise, as I mentioned, I think trademark owners simply have to be vigilant and always feel free to reach out to us if they think something may be amiss.

Lee: Well, thank you for this great conversation, Kevin.

Bovard: Thank you, Leeann. Great to be here.

Lee: If you have any questions for Kevin, his contact information is in the show notes. For more information on BakerHostetler's intellectual property perspectives thought leadership piece, we encourage you to download the document on bakerlaw.com. As always, thanks for listening to BakerHosts.