Fight the Explosion of Scammers Misusing Your Trademarks

April 7, 2020

Scammers have been quick to capitalize on COVID-19 fears and are using trademarks to do it. Fortunately, while the current climate requires vigilance, remedies are available.

Companies supplying personal protective equipment have been frequent targets of attack. Scammers are setting up websites under domain names containing the companies' famous brands. In some cases, the scammers also take photos or video from the brand owners' sites in an effort to legitimize their sites. The scammers then sell counterfeits, third party substandard products, or engage in price gouging.

A cease and desist letter may be enough to cause a bad actor to stop using the brand owner's mark and other IP, and start the process to get the domain name transferred. If the bad actor will not transfer the name voluntarily, the brand owner can follow up with a Uniform Dispute Resolution Policy ("UDRP") or Uniform Rapid Suspension ("URS") complaint before an appropriate forum, such as the National Arbitration Forum. These remedies are inexpensive and relatively quick, often resolving within approximately 90 days.

For serious infractions, companies can file for relief in federal court seeking temporary restraining orders and/or preliminary injunctions. Federal courts have procedures to handle emergency relief during the current crisis.

Price gougers may also be reported to their states' Attorneys General. Some states, such as Florida, have hotlines or other rapid response procedures for acting against price gouging. Companies are also setting up their own hotlines on which consumers can report price gouging.

Companies may file their own anti-counterfeiting actions, or work with law enforcement, which is increasingly active in this area. Interpol recently carried out Operation Pangea in which authorities from 90 countries took action against online sales of unlawful medical products and medicines. According to interpol.int, "[t]he seizure of more than 34,000 counterfeit and substandard masks, “corona spray”, “coronavirus packages” or “coronavirus medicine” reveals only the tip of the iceberg regarding this new trend in counterfeiting."

Amazon and other major on line retailers have take-down procedures for counterfeits. These require brand owners establish their intellectual property rights. Providing a

trademark registration is the easiest way to do this, so it is a good idea to review your portfolio for gaps and file new applications as necessary.

Domain name registrars are also trying to help eliminate fraud. After the New York Attorney General wrote to them on March 20, domain name registrars such as GoDaddy reportedly stepped up their efforts to combat COVID-19 related fraud. For example, Namecheap reportedly has removed words like “coronavirus,” “COVID,” and “vaccine” from its domain availability search tool.

Phishing, while always a popular scam, is exploding. Websites offering to expedite federal stipends are popular, as are false offers of free N-95 masks. Scammers also impersonate customer support, all in an effort to trick users into providing personal information or paying money for goods and services they will never receive. Insidiously, scammers may also send email that apparently comes from within your organization. They lure employees into clicking on a link, then install ransomware or other malware. When in doubt, do not click on a link. Report it to your IT manager, who should be able to spot the scam.

In short, many tools are available to help stem the tide of on-line fraud relating to COVID-19, from take-down requests through and including federal court litigation. For more information, please contact Janet Marvel at jam@pattishall.com.

Janet Marvel is a Partner of the firm, and Editor in Chief of the American Bar Association Intellectual Property Section magazine, LANDSLIDE®*.*