

Publication

03/07/2024

USPTO and Trademark Services Fraud Schemes

Scammers know no bounds, including in the world of trademarks. NGE has noted a recent uptick in fraudulent e-mails, calls, and texts directed at trademark applicants and registrants. These scammers typically use information about your brand to solicit personal information or steal money, often under the guise of registering your brand or “moving your application forward.” As a general rule, do not engage with anyone who claims to be from the U.S. Patent and Trademark Office (USPTO) or a private “registry” service; rather, decline the outreach and call or email your NGE attorney instead.

Here is what you need to know to protect yourself and your brand from fraudulent schemes and solicitation:

Scammers Use Accurate Information About Your Mark to Trick You

The USPTO’s search tools allow the public to find information about pending, registered, and dead trademarks and their owners, providing valuable information to anyone for free. However, this ease of access comes with an unfortunate downside—scammers can also use the USPTO’s records to obtain contact information for trademark applicants and registrants. Just because a message or caller has accurate information about your trademark, including your trademark’s application or registration number, upcoming deadlines, or your attorney’s name, does not mean they are

CLIENT SERVICES

Intellectual Property
Trademarks, Copyrights & Trade Secrets
Trademark Prosecution
Portfolio Management

RELATED PEOPLE

Michael G. Kelber
Alexandra Maloney

contacting you for a legitimate reason. Here is a recent email that is emblematic of this phenomenon (with the actual brand redacted):



Scammers Impersonate the USPTO Over the Phone or Text

Scammers often “spoof” or manipulate their caller ID to mask their identity and display a different name, number, and location. Unfortunately, this can even include spoofing the USPTO’s actual phone number. While you should not rely upon caller ID to tell if a call is legitimate, there are still other ways to detect a scam call. For example, USPTO employees will never ask for your credit card or social security number over the phone. The USPTO only accepts payment for trademark fees over its electronic filing system, so never provide your credit card or social security information over the phone, even if they say payment is “urgent” for your application to proceed.

Scammers Impersonate the USPTO Over E-mail

Scammers can also disguise their e-mail addresses and signature blocks to look like an official USPTO message. Official e-mails from the USPTO will always be from an “@uspto.gov” e-mail address—do not be fooled by similar e-mail addresses or a sender with “U.S.,” “Trademark,” “Patent,” “Registration,” or “Office” in the title. Here is an example:



Scammers Pose as Private Services

An alternate version of the scheme is for scammers to pose as a service that can help you register your mark,



respond to an Office Action, or renew your mark. Beware of any e-mail regarding your application sent from anyone other than your NGE attorney or official correspondence from an "@uspto.gov" e-mail address, especially if they ask for an immediate response. Below is an example:



Scammers Register Similar Domain Names

NGE has also noted an increased volume in domain name fraud, where scammers register domain names infringing on registered trademarks. The sites then masquerade as the business that owns the trademark to harvest personal and credit card information. They may register a name that includes a brand but change the domain extension from ".com" to ".net" or ".shop." Alternatively, they can modify the domain to be a confusingly similar name to the mark by misspelling or using substitute symbols, like a dash rather than a period, hoping unsuspecting customers will make purchases or provide personal information on the fake website. This scheme has been particularly prevalent in the hiring/HR context, unfortunately taking advantage of would-be job seekers.

If You Receive a Fraudulent Call or E-mail or Spot a Fraudulent Domain: hang up and do not respond to any of their messages.

Please also contact your NGE attorney before paying any fees or subscribing to any services—NGE's practice is to docket all communications from authorized Patent and Trademark Offices, including upcoming deadlines for



trademark applications, and will answer any questions you have about the process. For domain name fraud, do not engage with the website, and please contact your NGE attorney to take the next steps to remove the infringing website.

If you have any further questions about fraudulent trademark solicitation schemes and how to avoid them, please contact Michael Kelber, Alexandra Maloney, or your NGE attorney.

The content above is based on information current at the time of its publication and may not reflect the most recent developments or guidance. Neal Gerber Eisenberg LLP provides this content for general informational purposes only. It does not constitute legal advice, and does not create an attorney-client relationship. You should seek advice from professional advisers with respect to your particular circumstances.