

Client Alert | April 1, 2024

Morrison Cohen Cyber Watch: Navigating the Cyber Landscape Safely, Part One

The Marks of a Trademark Scam

Stay ahead of the game: unveiling scam tactics, spotting red flags and partnering with trusted advisors for comprehensive security

If you or your company holds a trademark application or registration, you may be a target for trademark scams. Threat actors may send you letters in the mail, or may contact you by phone, text or email, frequently using phone numbers, caller IDs or email addresses that spoof—or appear identical to—legitimate United States Patent and Trademark Office (USPTO) addresses or numbers.

The scams range from trying to induce you to pay fees that you don't actually owe or fees for services pertaining to your trademark application or registration that you don't need, or seeking sensitive personal information from you that they will then use nefariously or sell on the dark web. Some of the claims they might make include: (1) you have a bill or invoice due; (2) they can represent you before the USPTO; (3) your trademark filing was not processed correctly; (4) your trademark is pending cancellation; (5) a renewal or other filing is due to keep your trademark alive; or (6) a third party applied for a similar trademark to yours and you need to take action to protect your brand. The communications often look professional and polished and often indistinguishable from USPTO communications to the eyes of a layperson.

What can you do to protect your business? Consider the following examples and action items:

- The USPTO will send communications to you and the attorney of record only, but they never send invoices by mail or email, and they never make phone calls asking for money. All fees due to the USPTO need to be paid (usually up front, when filings are initially made) through the USPTO.gov website. If you receive something that looks like an invoice from the USPTO, it's likely fraudulent, and you should likely ignore it (or even better, not open it at all, to avoid a potential phishing attack!).
- The USPTO does not send letters via physical mail or facsimile and does not make phone calls notifying trademark owners of upcoming deadlines. If you receive one of these, it's likely a service provider seeking work (who may or may not have the qualifications and experience to make filings on your behalf), or a fraudster. Best to disregard these.
- Emails from a @uspto.gov domain may be real USPTO correspondence, but keep an eye out for typos or variations in the domain. Oftentimes, the underlying email address of the sender looks like a @uspto.gov address, but upon further inspection is clearly not (e.g., @usqto.gov). If you hover over the email address, you should be able to see the real sender to confirm.
- Also note that the USPTO will always copy your attorney on email correspondence, so leaving your attorney off the email can be a tell-tale sign that the email didn't actually come from the USPTO (assuming, of course, you have an appointed attorney). If you have an attorney of record appointed, and they were not copied on the correspondence, it's likely a fake.
- The USPTO always gives a reasonable amount of time to make filings (usually three to six months). Tight deadlines and a sense of urgency aimed to spur you into immediate action are usually a red flag. Best to disregard such messages, or send them to your attorney for confirmation of the next upcoming filing.
- Some fraudsters attempt to engage you in a conversation or seek for you to send money by claiming that they have been engaged by a third party to file a competing trademark application (often in a foreign country). A real trademark agent or attorney would not discuss their applications with third parties (especially ones who might have a claim of infringement against their client). Don't fall for this one!

- Offers for lifetime registration fees, offers to expedite your trademark registration process and offers to set up a USPTO.gov account on your behalf should all be suspect, and are best ignored.
- Claims that you are *required* to register your trademark with the USPTO are always false (trademark registration is not required by law, although often advisable depending on the circumstances).
- As with any scam, watch out for typos and grammatical errors in the correspondence you receive. The USPTO is meticulous about their correspondence and would not usually include any typos in their messages.

Key Contacts

Morrison Cohen's Technology, Data & IP team is available to assist clients with any questions regarding potential trademark scams, including confirming the legitimacy of a correspondence, verifying the next action to be taken with the USPTO or other foreign agency, and helping to report an incident to the USPTO.

Jessica L. Lipson
Partner & Co-Chair

D 212.735.8683
jlipson@morrisoncohen.com

Tess Bonoli
Associate

D 212.735.8728
tbonoli@morrisoncohen.com

Fred H. Perkins
Partner & Co-Chair

D 212.735.8647
fhperkins@morrisoncohen.com

Allison O'Hara
Associate

D 212.735.8807
aohara@morrisoncohen.com

The authors would like to extend their thanks to Morrison Cohen's Chief Information Security Officer, Thomas Catenaccio, for his invaluable contributions to this article.

This document is attorney advertising and is provided for informational purposes only as a service to clients and other friends. This document does not constitute legal advice. Reading or receiving this document does not create an attorney-client relationship, nor should the information in the document be deemed to be provided to you confidentially. Please contact one of our attorneys should you wish to engage Morrison Cohen LLP to represent you, so that an attorney-client relationship may be established between our Firm and you. Prior results do not guarantee a similar outcome.