

Bloomberg Law News 2023-06-12T15:48:34744453666-04:00

Trademark Office Data Leak Leaves Applicants Vulnerable to Fraud

By Riddhi Setty 2023-06-09T18:19:00000-04:00

- PTO said data security incident made public applicant addresses
- Attorneys express concern over applicant exposure to fraud

An accidental public reveal of some trademark applicants' addresses by the US Patent and Trademark Office puts these applicants at increased risk of receiving fraudulent notices, according to some attorneys.

The agency sent certain trademark attorneys and impacted customers a notification on Friday alerting them of a "data security incident" that resulted in public accessibility to some applicants' addresses, which are meant to be protected in private records.

According to the notice, a copy of which was reviewed by Bloomberg Law, the office discovered this issue in February and took down the impacted bulk data until it implemented a permanent fix at the end of March. The office then replaced the effected files with new versions that omit the addresses and fixed the issue causing data exposures.

"Since April 1, 2023, domicile addresses are properly masked, and all vulnerabilities have been corrected," the PTO said in its notice.

"Importantly, this incident was not the result of malicious activity, and we have no reason to believe that your domicile information has been misused," the notice added. "Nevertheless, we take all data security concerns seriously, and we apologize for our mistake."

The office instituted a requirement in 2019 that made it essential to include applicants' domicile addresses in trademark applications. In its notice about the data security issue, the office said this requirement helps them determine if a U.S.-licensed attorney is representing clients, which in turn helps them prevent fraudulent filings.

The PTO has implemented various measures over recent years to combat a [rapid increase](#) in

fraudulent trademark application filings. Already this year, it has issued at least four times as many sanctions for fraudulent or improper applicants as it did last year but continues to struggle with increasing fraudulent schemes. Some attorneys are concerned the data security issue might lead to further fraudulent activity.

Privacy Concerns

Some trademark attorneys said they protested the domicile address requirement when it was issued, raising safety concerns for their clients' data.

“When they first announced that they were going to add that requirement that was everyone’s biggest concern, how they’re going to keep it secret,” said [William Stroeve](#), an attorney at Cole Schotz P.C.

In 2021, trademark attorney [Pamela Chestek](#) of Chestek Legal filed a Trademark Trial and Appeal Board [opposition](#) to the PTO’s decision to reject a trademark application she had filed because it listed a P.O. box instead of a street address. When the TTAB sided with the agency, Chestek appealed to the US Court of Appeals for the Federal Circuit.

In a [letter](#) to acting clerk of court Jarrett Perlow on Friday, which included a copy of the notice, the PTO informed the court of the data security incident. It said the information doesn’t “call the TTAB’s decision into question” and that the office wished to correct the record.

“The PTO has betrayed applicants who trusted it to keep their sensitive personal information confidential, as PTO officials promised they were doing time and time again. That broken promise confirms the PTO’s complete disdain for individual privacy,” Chestek said in a statement to Bloomberg Law.

[Tara Aaron-Stelluto](#), a partner at Barton LLP, said Chestek received support within the trademark community when she filed her appeal.

“There was, I think, also some concern about whether or not the trademark office had the technology available to actually protect this information, and I think it may have been known for some time that some of these addresses were showing up in unexpected places like the bulk data,” said Aaron-Stelluto, who added that attorneys were “disappointed but not surprised” to learn of the data breach.

The PTO didn't immediately respond to a request for comment.

Possible Fraud Increase

Attorneys said the biggest concern with regard to clients' addresses being made public is increased exposure to fraudulent activities by bad-faith actors.

"What we've seen as a result, I believe, of the data breach but also just generally is that our clients are getting even more spam phone calls, texts, mail, you name it, from any number of these fraudulent entities," said [Monica Riva Talley](#), director of Sterne, Kessler, Goldstein & Fox PLLC's trademark and brand protection practice.

Talley said "not a day goes by" where a client doesn't send her a scam notice they've received asking if any action is required of them for their trademark registration application.

Aaron-Stelluto said while fraudulent notices are already rampant, "this just raises the risk that more of those notifications are going to be able to go out and the companies that are doing that can do it more efficiently."

"There's a clear risk of harm," she said, "and I think the trademark office took that into account when deciding whether or not to put these notices out and they're certainly going to get some angry notices from trademark attorneys who say we told you that this was going to happen, but I think they deserve credit for making it public."

To contact the reporter on this story: Riddhi Setty in Washington at rsetty@bloombergindustry.com

To contact the editors responsible for this story: James Arkin at jarkin@bloombergindustry.com; Jay-Anne B. Casuga at jcasuga@bloomberglaw.com

Related Articles

[Surge in Trademark Fraud Scams Overwhelms Regulators, Applicants](#)

Related Documents

[Letter to Federal Circuit](#)