
October 15, 2025

Daniel Lee,
Assistant U.S. Trade Representative for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street, NW
Washington, D.C. 20508

Re: Rebuttal comments regarding the Request for public comment on the 2025
Review of Notorious Markets for Counterfeiting and Piracy: Comment Request
USTR-2025-0018

Dear Mr. Lee,

We write in response to the Office of the United States Trade Representative's request for rebuttal comments concerning the 2025 Review of Notorious Markets for Counterfeiting and Piracy. As in past cycles, a small number of rightsholder groups have referenced Cloudflare in their submissions. We find it necessary to respond because these comments not only contain mischaracterizations regarding the nature of Cloudflare's services but also advocate for new policy actions and approaches entirely unrelated to "identif[ying] examples of online and physical markets that reportedly engage in and facilitate substantial copyright piracy or trademark counterfeiting that infringe on U.S. intellectual property."¹ We firmly believe that the continued use of the Notorious Markets process to pressure Cloudflare and other Internet infrastructure companies into taking actions neither expected nor required by U.S. law is both misguided and a misuse of this vital trade tool.

¹ Office of United States Trade Representative, 2025 Review of Notorious Markets for Counterfeiting and Piracy: Comment Request, 90 FR 40135 (Aug. 18, 2025).

We are submitting these comments to provide additional background on Cloudflare as well as actions we have taken with rightsholders, including some of those who filed comments.

I. Background on Cloudflare

Cloudflare, Inc. is the leading connectivity cloud company that runs one of the world's largest networks providing security, performance, and reliability services to millions of Internet properties, such as websites, network and other applications online. Cloudflare powers Internet requests for more than 36% of the Fortune 500 and serves over 84 million HTTP requests per second on average. Cloudflare interconnects with approximately 13,000 networks globally, including major Internet Service Providers (ISPs), cloud services, and enterprises.

Cloudflare offers a wide variety of services to improve the security, reliability, and performance of online web properties. Cloudflare's website security services work by directing web visitor traffic to Cloudflare's network rather than directly to the website's hosting provider. Cloudflare then uses its "points of presence" in more than 330 cities in over 125 countries to screen traffic for cybersecurity risks and to cache content at the network edge in order to improve website performance. Although Cloudflare does offer certain web hosting services to a limited number of sites,² only one of the publicly available responses that reference Cloudflare alleges that we host the websites that they complain about. The commenter is not only mistaken, but it lists the actual host in its comment, thereby acknowledging that we are not the actual host. The other organizations merely note that certain websites use our security and caching services or otherwise make vague references to our services.

Cloudflare is dedicated to improving the security, performance, and reliability of anything connected to the Internet. Indeed, the U.S. District Court for the Northern

² The number of takedown notices that Cloudflare has received for content stored on our network is exceedingly small. See Cloudflare Transparency Report, available at <https://www.cloudflare.com/transparency/>. When we do receive takedown notices, Cloudflare conducts notice and takedown procedures, consistent with the requirements of the Digital Millennium Copyright Act (DMCA).

District of California concluded that Cloudflare’s security and caching services do not “materially contribute” to or “significantly magnif[y]” copyright infringement, observing that “removing material from a cache without removing it from the hosting server would not prevent the direct infringement from occurring” and “[f]rom the perspective of a user accessing the infringing websites, these services make no difference.”³

To further our mission to “help build a better Internet,” Cloudflare makes many of our cybersecurity and performance services widely available for free or at a low cost. Our free and low cost services to protect websites and applications from malicious cyberattacks are used around the globe. Our customers include every type of organization, from Fortune 500 companies and government institutions to small businesses, non-governmental organizations, and personal blogs. The broad availability of Cloudflare’s services helps mitigate the risk posed by malicious cyber activities, improves the reliability and performance of the Internet for everyone online, and provides developers with a reliable platform to build and deploy innovative solutions globally through our edge network. The result of all of the above is that we provide our services at a very significant scale, for tens of millions of domains: more than 20 percent of web sites behind Cloudflare’s network.

II. Cloudflare’s abuse process

Cloudflare’s services are vital to the security, reliability, and performance of the Internet, and we take our legal obligations seriously, acting responsibly to assist rightsholders. Cloudflare has a robust abuse reporting system that allows rightsholders to report allegations of copyright infringement across the millions of websites using our services. Our system is explicitly designed to ensure complainants are in the same position they would be if the website did not use our services: we ensure they have the information necessary to report alleged infringement to the party with the sole power to remove the content from the

³ See *Mon Cheri Bridals, LLC v. Cloudflare, Inc.*, Case No. 19-cv-01356-VC (N.D. Cal. Oct. 6, 2021) available at https://assets.ctfassets.net/slt3lc6tev37/7gr79MdC7Wnb3zbVzJoRzP/507d581550d04e7ac7a7f71d3c0a6715/2021_10_06_-151_0-ORDER_by_Judge_Vince_Chhabria_Den_124_Pls_MSI_granting_133_Def_s_MSI_Further_Case_Management_1.pdf.

web—the website hosting provider. Our semi-automated abuse system passes on allegations of copyright violations to both the website owner and their hosting provider, enabling appropriate action. Concurrently, Cloudflare directly provides complainants with the hosting provider's contact information, facilitating necessary direct follow-up.

Given the function of our abuse reporting system, the use of Cloudflare services does not fundamentally impair a rightsholder's ability to identify and access a website's hosting provider. To obtain the necessary hosting provider information, a rightsholder simply needs to submit a copyright complaint through our abuse web form. In fact, and consistent with previous years, the rightsholders who referenced Cloudflare in their complaints also referenced the hosting providers for those same websites. This outcome clearly demonstrates Cloudflare's cooperation in providing them with the timely information required to pursue effective takedown actions.

Cloudflare does not generally publicly disclose sensitive origin host IP address information for websites using its services, and this policy is essential for strong cybersecurity. Disclosing this data would allow—and historically has allowed—malicious actors to bypass Cloudflare's security protections and directly attack the underlying website. While we recognize the importance of addressing copyright infringement, we firmly believe that exposing a website to a cyberattack is neither an appropriate nor a legally acceptable method for resolving an intellectual property dispute.

III. Cloudflare's work with rightsholders

Cloudflare operates a Trusted Reporter program that provides access to origin host IP addresses for entities demonstrating a genuine, verified need for the information. To qualify, these entities must prove a commitment and capability to secure the data and prevent its misuse for cyberattacks. The program is utilized by a variety of major industry groups representing intellectual property rightsholders, including the MPA (Motion Picture Association) and the RIAA (Recording Industry

Association of America). Cloudflare has on-boarded over 350 organizations and agencies into the Trusted Reporter Program.

Over the past few years, Cloudflare has invested in developing innovative tools to speed up the processing of critical information. Recognizing the need for efficiency, we built an API that enables entities to automate their submissions to Cloudflare's reporting form, leveraging automation to facilitate processes where appropriate. This program ensures that information is handled quickly and effectively. The API allows organizations to send abuse reports to Cloudflare in an automated way without having to enter relevant information manually into Cloudflare's abuse form. Nearly 60 of the entities in our Trusted Reporter Program make use of the API abuse reporting form.

Cloudflare offers additional resources beyond our standard abuse reporting to assist rightsholders investigating possible infringement. Specifically, we provide information in response to appropriate legal process, such as subpoenas issued under the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(h). We maintain that it is not appropriate to release the sensitive personal information of our users to *any* third party—including a rightsholder group—without valid legal process. This private user information is protected by privacy laws around the world and must not be transferred simply upon request.

Cloudflare remains actively engaged with lawmakers, industry groups, regulatory bodies, and law enforcement to collaboratively explore and implement additional, effective steps to address concerns regarding online infringement.

IV. Conclusion

Cloudflare's security services are essential for improving the overall security and performance of the Internet and do not materially contribute to or substantially magnify copyright infringement. We maintain that it's time for rightsholders to shift their focus away from policy advocacy targeting Internet infrastructure and instead

concentrate on the physical and online markets that are the intended subject of the Notorious Markets report.

Cloudflare remains committed to acting responsibly and thoughtfully to assist rightsholders in a manner consistent with the services we provide. We look forward to engaging in further discussions with you and other stakeholders to collaboratively identify effective, infrastructure-consistent ways to address online infringement.

Sincerely,

/s/ Zaid A. Zaid

Zaid A. Zaid
Director, Head of U.S. Public Policy