UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

DENIECE WAIDHOFER, an individual; MARGARET MCGEHEE, an individual; and RYUU LAVITZ, LLC, a Massachusetts limited liability company,

Plaintiffs,

v.

CLOUDFLARE, INC., a Delaware corporation; BANGBROS.COM, INC., a Florida corporation; SONESTA TECHNOLOGIES, INC., a Florida corporation; MULTI MEDIA LLC, a California limited liability company; CRAKMEDIA INC., a Canadian corporation; and JOHN DOES 1-21, as-yet unidentified individuals,

Defendants.

Case No. 2:20-cv-06979

PLAINTIFFS' RESPONSE TO DEFENDANT CLOUDFLARE'S MOTION FOR SANCTIONS PURSUANT TO RULE 11 AND COUNTERMOTION

Judge: Hon. Fernando M. Olguin
Date: January 28, 2021
Time: 10:00 AM PST
Place: Courtroom 6D – 6th Floor
350 W. 1st Street
Los Angeles, CA 90012

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

RULES

OTHER AUTHORITIES

Plaintiffs hereby respond to Defendant Cloudflare Inc.'s ("Cloudflare") Motion for Sanctions Pursuant to Rule 11 (the "Motion" or Dkt 102) and countermove for Rule 11 sanctions against Cloudflare (the "Countermotion").

INTRODUCTION

Based solely on Cloudflare's and its counsel's *unsworn*, *untested*, and *unsubstantiated* denials of the so-called Argo Tunnel allegations, Cloudflare contends that Plaintiffs should be sanctioned under Rule 11. Cloudflare accuses Plaintiffs' counsel of failing to conduct a reasonable investigation and failing to provide evidence for its allegations. But Cloudflare itself has not served any discovery requests to ascertain the basis for the Argo Tunnel allegations through legitimate processes in accordance with the Rules, and the Motion provides no explanation or evidence whatsoever regarding Cloudflare's own investigation (if any) or the factual basis (if any) for its Argo Tunnel denials. Rather, Cloudflare contends that Plaintiffs must divulge the results of their prefiling investigation (including privileged communications and work product) in response to Cloudflare's counsel's baseless and insulting accusations impugning Plaintiffs' counsel's integrity and professionalism, simply because Cloudflare and its counsel baldly assert the Argo Tunnel allegations are false. Because the Motion is frivolous and apparently lodged for an improper purpose to circumvent discovery, obtain privileged information, drive up litigation costs, and delay, distract, harass, and intimidate Plaintiffs, it should be denied and Cloudflare should be sanctioned.

The First Amended Complaint ("FAC") contains 342 paragraphs and nearly 90 pages of detailed factual allegations showing rampant copyright piracy directed at OnlyFans and Patreon creators on Thothub, home to an alleged criminal enterprise that was Cloudflare's paying customer until the site shut down in the wake of this lawsuit. In painstaking detail that reflects the rigorous factual

investigation that preceded it, the FAC alleges how the Thothub organization operated, how it recruited new members to steal copyrighted paywall-protected works from creators like Plaintiffs, and how it distributed those works to millions of its members and visitors. In equally rigorous detail, the FAC explains how Cloudflare—an unscrupulous CDN provider that routinely supports and enables online pirates—knowingly facilitated this criminality for years, despite receiving hundreds of notices from aggrieved creators, including all three Plaintiffs.

Cloudflare's conduct, as alleged in the FAC, is appalling. Among other things, the FAC alleges that, for a price, Cloudflare enabled Thothub's distribution of infringing works, stored infringing works, and allowed Thothub to operate on a vast scale by offloading heavy user traffic. It alleges that Cloudflare has carved out a competitive niche by serving illegal pirate sites that other large CDN companies would not, and that Cloudflare provides services for about 40% of all pirate sites, about 62% of the top 500 infringing domains, and about 45% of all infringing URLs reported in 2019. It alleges that Cloudflare regularly caters to pirates for business reasons and markets to pirates by, for example, promoting protection from copyright owners and law enforcement. It alleges that Cloudflare received hundreds of notices from OnlyFans and Patreon creators (including the three Plaintiffs) related to Thothub, yet continued to serve Thothub and known infringing URLs. It alleges that Cloudflare obfuscated its role by deleting copies of Plaintiff Waidhofer's works from its servers then denied ever having made such copies, all while continuing to serve infringing copies. It alleges that Cloudflare continues to serve many other sites similar to Thothub, including a direct copycat. And it alleges that Cloudflare spurns reasonable measures to prevent repeat infringement, does not follow up on infringement notices, and (despite routinely

doing business with so many pirates) has never voluntarily terminated the account of a repeat infringer.

But Cloudflare does not complain in its Rule 11 motion about any of those allegations. Instead, Cloudflare's motion identifies one discrete set of allegations that Cloudflare asserts (without *any* evidence other than its own uncorroborated, self-serving statements) are false. These allegations relate to Cloudflare's apparent provision of a service called "Argo Tunnel" that "creates an encrypted tunnel between [the customer's] origin web server and Cloudflare's nearest data center—all without opening any public inbound ports." In layman's terms, the Argo Tunnel blocks users from accessing a Cloudflare customer's home servers directly at its unique IP address and instead routes all user traffic exclusively through Cloudflare's network. As explained below, the FAC's allegations regarding the Argo Tunnel—like all of its other allegations—have a reasonable basis backed by evidence resulting from Plaintiffs' counsel's diligent investigation regarding relevant facts and law, which began months before suit and continues to this day. The Argo Tunnel allegations, in particular, are supported by expert analysis, as well as statements on Thothub and on Cloudflare's own website.

The Motion falls far short of the high standard for imposing chilling sanctions under Rule 11, particularly in the context of the well-pleaded complaint. Instead, the Motion reflects an improper use of Rule 11 to emphasize Cloudflare's positions on the merits, intimidate an adversary into withdrawing contentions that are (at minimum) fairly debatable, increase the costs of litigation, seek disclosure of information (which includes privileged communications and work product) outside the bounds of discovery, and harass, distract, and burden less-resourced opponents. *Cf. Walker v. Blackground Records, LLC*, 2017 WL 8186040 (C.D. Cal. Aug. 7, 2017) (Olguin, J.) (sanctioning defendants for filing a "frivolous"

Rule 11 motion "for an improper purpose"). In light of Cloudflare's tactical abuse of Rule 11, the Court should deny the Motion and appropriately sanction Cloudflare and its counsel.

FACTUAL BACKGROUND

Plaintiff Deniece Waidhofer filed the original complaint in this action on August 3, 2020, including copyright, RICO, and negligence claims against Cloudflare. (Dkt 1). After defendants filed motions to dismiss, plaintiffs filed an amended complaint (the FAC) as of right within the period allowed by Rule 15(a)(1)(B). (Dkt 68). The FAC added two new plaintiffs (McGehee and Ryuu Lavitz LLC) and two new defendants (CrakMedia, Inc. and Sonesta Technologies, Inc.). (*Id.*) In addition, among other revisions, the FAC dropped some claims and asserted only direct and contributory copyright claims against Cloudflare. (*Id.*)[1]

Among other additional factual allegations, the FAC included allegations regarding Cloudflare's so-called "Argo Tunnel" service, which allegedly creates an encrypted tunnel between Cloudflare's customer's servers and Cloudflare's nearest data center, thereby routing all traffic through Cloudflare's network and preventing direct access to the customer's servers even if a user knows the customer's server's unique IP address. (*See* FAC ¶¶ 203–05). Cloudflare's motion does not dispute that it offers the Argo Tunnel service or that the Argo Tunnel service operates as described; indeed, this information was gleaned from Cloudflare's own website. (*See* Ex. 2A at App. 19–22; Ex. 2B at App. 30). However, the FAC further alleges, "[o]n information and belief," that Cloudflare set up an Argo Tunnel for Thothub and that Cloudflare could have thus prevented all user access to infringing works

[1] Plaintiffs elected not to pursue the RICO and negligence claims against Cloudflare in the FAC based on strategic considerations that are protected from disclosure as work product, not because Plaintiffs believed these allegations were unfounded, as the Motion insinuates.

on Thothub by closing this tunnel, which Cloudflare denies. (*See* FAC ¶¶ 206–07, 9).

The Argo Tunnel allegations have a firm basis in evidence. Most notably, prior to filing the FAC, Plaintiffs' counsel conferred with Thomas "Damien" Bell. (*See* Rosenthal Decl., Ex. 2, ¶ 8). Mr. Bell is an expert in information and network technology with extensive experience regarding computer programming and network operations. (*See* Bell Decl., Ex. 1, ¶¶ 1–6). Among other relevant experience, Mr. Bell worked as a technical support engineer for Akamai Technologies, Inc., a leading CDN provider, where he was responsible for investigating hacking attempts for Fortune 500 companies; utilized cutting-edge network tools to ensure platform availability, reliability and security for customers; employed networking techniques to analyze traffic across https, VPN, and international networks; and utilized WireShark programs to investigate packet loss and other anomalous network traffic. (*Id.* ¶ 3). Mr. Bell has extensive expertise in technical matters such as networking, including TCP/IP, DNS, VPN, CDN, and network subnetting; tools and macros, including Python, AutoHotKey, AutoIt, and JavaScript; protocols, including Telnet, SSH, SFTP, HTTP, and HTTPS; environments, including Windows, Linux, and Mac; programming languages, including C++, Java, CSS3, HTML5, MySql, MongoDB, JavaScript, Python, and PHP; and techniques and concepts, including APIs and microservices, CDN, and virtualization. (*Id.* ¶ 4). Mr. Bell currently works as an employee handling system administration and content rights management for Plaintiff Ryuu Lavitz LLC, where (among other things) he assists in protecting the company's intellectual property from infringement using advanced techniques to track piracy. (*Id.* ¶ 2).

Due to ongoing infringement of Ryuu Lavitz's copyrights on Thothub, Mr. Bell began investigating Thothub in early 2020. (*Id.* ¶¶ 7–8). Using unique Google

Analytics identifiers for Thothub's main pages (the "Main Site") and forums (the "Forums") and a specialized search engine called Shodan.io, Mr. Bell discovered that the Main Site and Forums were hosted at two separate IP addresses. (*Id.* ¶¶ 9–11). Mr. Bell then checked the accuracy of these IP addresses by setting up a customized http request known as a "CURL request," which contacted the identified IP addresses using the domain name as a header to confirm a chain of custody to a specific web-hosting provider (rather than through a proxy like Cloudflare). (*Id.* ¶¶ 12–14). Mr. Bell further validated the IP addresses using DNS Trails (a repository of historical DNS data) through a web service called SecurityTrails. (*Id.* ¶ 16). In layman's terms, this process confirmed that Mr. Bell had correctly identified the online location of Thothub's home servers and could directly access them, while bypassing Cloudflare's intermediary (proxy) server network.

Over the next few months, Mr. Bell re-tested the aforementioned CURL requests on several occasions and received the same results. (*Id.* ¶ 17). However, on or around June 1, 2020 when he again attempted the CURL request for the Forums, the request did not return the requested pages. (*Id.* ¶ 17). Instead, for the first time, a *Cloudflare*-branded error message entitled "Error 1003" appeared, with a notation stating "Error 1003 Access Denied: Direct IP Access Denied." (*Id.* ¶¶ 17–18). In other words, the Forums' server could no longer be directly accessed at its IP address and instead Cloudflare was apparently denying direct access to the server. Based on independent research, Mr. Bell learned that this error message indicated that the site could be using an Argo Tunnel. (*Id.*) Mr. Bell further tested this hypothesis by running a Linux-based program called "nmap," which is a network scanner used to discover hosts and services on a computer network by sending data packets and analyzing responses. (*Id.* ¶ 19). Using this program, Mr.

Bell learned that the Forums' server was utilizing a particular port (Port 8443) often used to implement an Argo Tunnel. (*Id.*) Based on this information, Mr. Bell concluded that Thothub was likely utilizing an Argo Tunnel or similar Cloudflare service to block direct public access to the Forums' server. (*Id.* ¶ 20).

Plaintiffs' counsel first met Mr. Bell and learned about his analysis of Thothub's operations after the date of the original complaint. (Ex. 2, ¶ 8). Counsel believed (and still believes) that, given Mr. Bell's technical experience and sophisticated analysis, his opinion is highly credible. (*Id.* ¶ 8) In addition, counsel observed that Mr. Bell's finding that Thothub's Main Page and Forums had separate IP addresses was further supported by written statements of Thothub's apparent chief operator, "Teller," who stated in a June 19, 2019 message that he had "put in a request for another round of server upgrades (*double the forum power and double the main website power*)." (Ex. 2C at App. 32) (emphasis added).[2] Counsel found further support for Mr. Bell's conclusions in Cloudflare's own statements on its website explaining the function and purpose of an Argo Tunnel, such as that "Argo Tunnel provides a secure way to connect your origin [server] to Cloudflare without a publicly routable IP address" and that the Argo Tunnel ensures that "only inbound web traffic through Cloudflare's network ever reaches your applications origin servers." (Ex. 2A at App. 22; Ex. 2B, at App. 30). Given this (and other) evidence, counsel included the Argo Tunnel allegations in the FAC and, in an abundance of caution because the allegations could not be verified absent discovery, expressly identified them as made "[o]n information and belief." (Ex. 2, ¶ 10).

[2] These facts are in tension with representations by Cloudflare's counsel (without evidentiary support) that the Forums were simply a "subdomain" of the Main Site. (Mot. at 7).

On October 15, 2020, Plaintiffs served an initial round of discovery requests on Cloudflare, including requests for production ("RFPs"), interrogatories, and requests for admission ("RFAs"). (Ex. 2, ¶ 13). Cloudflare asserted a string of meritless objections to the RFPs—for example, Cloudflare objected (without any reasonable explanation or evidence) that the term "agreement" was somehow vague, ambiguous, and unduly burdensome and that the distinctive search term "Thothub" was also somehow vague, ambiguous, unduly burdensome, and overly broad (again without explanation or evidence)—and to this day still has not produced a single document. (Cloudflare's RFP Responses, Ex. 2E, App. 67–79; *see also* Plaintiffs' Deficiency Letter, Ex. 2D, App. 40–66).[3] Cloudflare also responded to an RFA about Argo Tunnel by denying the allegations, while curiously redefining the term "Thothub" to refer only to the Main Site and not the Forums. (Dkt 102-3 at 4).

Three days later, on November 18, 2020—despite not having itself served any discovery requests or provided any documents in response to Plaintiffs' requests for production that were served on October 15—Cloudflare's counsel sent Plaintiffs' counsel a letter threatening Rule 11 sanctions. (Dkt 102-4 at 2–4). With no evidence or explanation and without having issued discovery requests of its own, Cloudflare's counsel simply asserted that a "reasonable investigation by Plaintiffs would have revealed that they have no factual basis for their [purportedly] false allegations that the thothub.tv website used Cloudflare's Argo Tunnel service or that Cloudflare 'set up an Argo Tunnel' for the thothub.tv website." (*Id.* at 4). The letter ended by warning that Cloudflare would bring a Rule 11 motion if Plaintiffs did not "either explain the basis for the purported

[3] Plaintiffs intend to bring a motion to compel imminently, though (as Cloudflare may have intended) they have been delayed in doing so by the necessity of responding to the Motion.

reasonable basis [*sic*] for [Plaintiffs'] belief, or confirm that [Plaintiffs] will withdraw these allegations." (*Id.*)

Plaintiffs' counsel responded to these accusations by explaining that he had "conducted a substantial, in-depth investigation into the relevant facts and law in this case, far more (I suspect) than any of the Defendants' counsel have done." (Dkt 102-5 at 2). Counsel noted that "Plaintiffs do not have an obligation to disclose details about the conduct or results of our factual investigation, including our discussions with consulting experts, simply because Defendants baldly assert the allegations are false." (*Id.*) Counsel further noted that Cloudflare had "done nothing to investigate the factual basis for Plaintiffs' allegations in accordance with the rules" and "have not served any discovery requests at all." (*Id.* at 2–3). Thus, counsel explained, the threatened Rule 11 motion "would itself be sanctionable." (*Id.* at 3). Finally, counsel pointed out Cloudflare's "misleading and evasive" RFA response "on exactly the point you now threaten Rule 11 sanctions," and requested that Cloudflare or its counsel swear "under oath" that "Cloudflare never provided Argo Tunnel services with respect to thothub.tv, forum.thothub.tv, or any other URLs associated with these web domains." (*Id.* at 3). In response, Cloudflare's counsel asserted (unsworn and without evidence) that "Cloudflare did not provide Argo Tunnel services to the thothub.tv website," which "includes any subdomains for the thothub.tv website." (Dkt 102-6 at 3–4). Later, Cloudflare's counsel represented (again without proof) that the Forums were a "subdomain" of the Main Site. (*Id.* at 2).

In a subsequent email, Plaintiffs' counsel advised Cloudflare's counsel to "ask your clients what Cloudflare Error 1003 is" and to "conduct due diligence on

the veracity of your client's representations." (*Id.* at 3).[4] Moreover, Plaintiffs' counsel again informed Cloudflare that "Plaintiffs have a good-faith basis for the referenced allegations based on multiple sources of information obtained during a diligent investigation, and the allegations are supported by specific facts both pled and unpled." (Ex. 2F at App. 81). Counsel further advised that the "threatened motion would be a highly improper use of Rule 11 as a discovery weapon" and that it "lacks a good-faith basis and does not come close to meeting Rule 11's standards." (*Id.*) "For instance," counsel noted, "the only purported evidence cited in support of Cloudflare's assertions regarding the underlying factual dispute is Cloudflare's own untested statements and discovery responses," and the referenced allegations "constitute just two paragraphs out of a 300-plus-paragraph complaint that spans nearly 90 pages." (*Id.*) Further, counsel noted that the Argo Tunnel "allegations—while certainly supportive of Plaintiffs' claims—are not vital to Plaintiffs' liability theories" (*id.*), as explained more fully in Plaintiffs' response to Cloudflare's motion to dismiss the contributory-infringement claims. (*See* Dkt 93 at 24–25).

Regardless, Cloudflare filed the Motion on December 29, 2020. (Dkt 102). On December 30, Plaintiffs' counsel offered Cloudflare until January 4 to withdraw the Motion and referred Cloudflare's counsel to this Court's decision in *Walker v. Blackground Records, LLC*, 2017 WL 8186040 (C.D. Cal. Aug. 7, 2017), in which the Court sanctioned defendants for bringing a "frivolous" Rule 11 motion regarding certain allegations in plaintiffs' complaint for an "improper purpose." (Ex. 2G at App. 82). Cloudflare did not respond and did not withdraw the Motion.

[4] Cloudflare chastises Plaintiffs for this comment by stating that "[c]alling one's litigation opponent a liar is not evidence of any kind." (Mot. at 12 n.4). This is an odd thing to say in the context of a motion that revolves *entirely* around calling one's litigation opponent a liar.

LEGAL STANDARDS

"Imposing sanctions under Rule 11 is an extraordinary remedy, one to be exercised with extreme caution.'" *Lee v. POW! Entm't, Inc.*, 468 F. Supp. 3d 1220, 1230–31 (C.D. Cal. 2020) (quotation omitted). "Rule 11 is intended to deter baseless filings in district court and imposes a duty of 'reasonable inquiry' so that anything filed with the court is well grounded in fact, legally tenable, and not interposed for any improper purpose." *Islamic Shura Council of S. Cal. v. Fed. Bureau of Investigation*, 757 F.3d 870, 872 (9th Cir. 2014) (per curiam) (internal quotation omitted). "One of the fundamental purposes of Rule 11 is to reduce frivolous claims, defenses or motions and to deter costly meritless maneuvers, thereby avoiding delay and unnecessary expense in litigation." *Walker v. Blackground Records, LLC*, 2017 WL 8186040, *4 (C.D. Cal. Aug. 7, 2017) (Olguin, J.) ("*Walker*") (quoting *Christian v. Mattel, Inc.*, 286 F.3d 1118, 1127 (9th Cir. 2002)). "Among other grounds, a district court may impose Rule 11 sanctions if a paper filed with the court is for an improper purpose, or if it is frivolous." *Id.* (quoting *G.C. & K.B. Invs., Inc. v. Wilson*, 326 F.3d 1096, 1109 (9th Cir. 2003)).

"When 'a complaint is the primary focus of Rule 11 proceedings, a district court must conduct a two-prong inquiry to determine (1) whether the complaint is legally or factually baseless from an objective perspective, and (2) if the attorney has conducted a reasonable and competent inquiry before signing and filing it.'" *Id.* (quoting *Holgate v. Baldwin*, 425 F.3d 671, 676 (9th Cir. 2005)). "As shorthand for this test, courts use the word 'frivolous' to denote a filing that is both baseless and made without a reasonable and competent inquiry." *Id.* (quoting *Holgate*). The applicable standard for prefiling inquiry is "one of reasonableness under the circumstances." 1983 Adv. Cmte. Note to Fed. R. Civ. P. 11 ("1983 Cmte.

Notes"); *see also In re Outlaw Lab., LP Litig.*, 2019 WL 3858900, *2 (S.D. Cal. Aug. 15, 2019) ("[T]he issue in determining whether to impose sanctions under Rule 11 is whether a reasonable attorney, having conducted an objectively reasonable inquiry into the facts and law, would have concluded that the offending paper was well-founded.") (quotation omitted). This lenient standard ensures that the rule does not "chill an attorney's enthusiasm or creativity in pursuing factual or legal theories." 1983 Cmte. Notes. "The rule does not require a party or an attorney to disclose privileged communications or work product in order to show that the signing of the pleading, motion, or other paper is substantially justified." *Id.*

Rule 11's provisions regarding factual contentions recognize "that sometimes a litigant may have good reason to believe that a fact is true or false but may need discovery, formal or informal, from opposing parties or third persons to gather and confirm the evidentiary basis for the allegation." 1993 Adv. Cmte. Notes to Fed. R. Civ. P. 11 ("1993 Cmte. Notes"). As such, the rule expressly permits factual contentions that "will likely have evidentiary support after a reasonable opportunity for further investigation or discovery." Fed. R. Civ. P. 11(b)(3). The "certification is that there is (or likely will be) 'evidentiary support' for the allegation, not that the party will prevail with respect to its contention regarding the fact." 1993 Cmte. Notes. A party can meet this standard even if it ultimately loses summary judgment. *Id.* "On the other hand, if a party has evidence with respect to a contention that would suffice to defeat a motion for summary judgment based thereon, it would have sufficient 'evidentiary support' for purposes of Rule 11." *Id.*

"As under former Rule 11, the filing of a motion for sanctions is itself subject to the requirements of the rule and can lead to sanctions." *Walker*, *supra*, at *8 (quoting 1993 Cmte. Notes). "The court may award to the person who prevails

on a motion under Rule 11—whether the movant or the target of the motion—reasonable expenses, including attorney's fees, incurred in presenting or opposing the motion." *Id.* (quoting 1993 Cmte. Notes); *see also* Fed. R. Civ. P. 11(c)(2). "A party defending a Rule 11 motion need not comply with the [rule's] separate document and safe harbor provisions when counter-requesting sanctions." *Patelco Cred. Union v. Sahni*, 262 F.3d 897, 913 (9th Cir. 2001). In assessing the propriety of a Rule 11 motion, the Court should bear in mind that Rule 11 "should not be employed as a discovery device or to test the legal sufficiency or efficacy of allegations in the pleadings … [n]or should Rule 11 motions be prepared to emphasize the merits of a party's position, to exact an unjust settlement, to intimidate an adversary into withdrawing contentions that are fairly debatable, to increase the costs of litigation, … or to seek disclosure of matters otherwise protected by the attorney-client privilege or the work-product doctrine." 1993 Cmte. Notes.

ARGUMENT

I. Cloudflare's Rule 11 Motion Is Frivolous.

The Motion does not come close to meeting the extraordinary standard to show that the Argo Tunnel allegations are legally or factually baseless, *nor* that the allegations were made without a reasonable and competent inquiry by Plaintiffs' counsel. *See Walker*, at 4 (quoting *Holgate v. Baldwin*, 425 F.3d 671, 676 (9th Cir. 2005)) (explaining that both of these points must be shown to support sanctions based on allegations in a complaint). On the contrary, the record shows that these allegations are amply supported by specific evidence, that additional evidentiary support is likely to emerge through discovery, and that Plaintiffs' counsel conducted a diligent investigation before filing the FAC. On the other hand, the

only support offered for Cloudflare's Motion is Cloudflare's and its counsel's entirely unsubstantiated assertions and denials. The Motion is therefore frivolous.

Each of the specific allegations disputed by Cloudflare is objectively reasonable and supported by evidence. *First*, Cloudflare contends that the "FAC falsely alleges" that "Cloudflare set up an Argo Tunnel for Thothub." (Mot. at 4). But Cloudflare concedes (as its own website proclaims) that "Cloudflare offers a security service it calls the 'Argo Tunnel,' which encrypts data as it moves between a customer's origin web server and Cloudflare's nearest data center." (*Id.*) Moreover, Mr. Bell used advanced technical analysis to identify Thothub's IP addresses, confirmed those IP addresses through multiple means, then later received a *Cloudflare*-branded error message (Error 1003) indicating direct access was denied at those addresses. (Ex. A, ¶¶ 10–21).[5] Mr. Bell further found that this error message is associated with an Argo Tunnel and that Thothub's forum server was utilizing the particular port often used to implement an Argo Tunnel. (*Id.* ¶ 20). This evidence provides more than a reasonable basis for the Argo Tunnel allegations.

In support of the Motion, Cloudflare offers *no evidence* and just asserts that the Argo Tunnel allegations are "simply false." (Mot. at 5). Later, Cloudflare bizarrely argues that "the only evidence available *conclusively shows* that Cloudflare did not provide Argo Tunnel service to Thothub." (*Id.* at 12, emphasis added). What evidence? Cloudflare produces no documentation or other admissible evidence in support of its assertion, instead relying entirely on *its own RFA response denying the allegations* (caveated by its myriad objections and redefinition of key terms) and its attorney's unsworn, unsupported emails that purportedly "confirm[] that Cloudflare did not provide Argo Tunnel services to the

[5] Cloudflare's Motion references a Cloudflare webpage that expressly defines this error code as "Error 1003 Access Denied: Direct IP Access Not Allowed." (Mot. at 13 n.6).

thothub.tv website, or to *any* of Thothub's subdomains." (*Id.*) Cloudflare's argument tortures the language and logic of Rule 36, which provides that an *admission* in response to an RFA "conclusively establishe[s]" a matter; the same conclusion obviously does not apply for a *denial* in response to an RFA. *See* Fed. R. Civ. P. 36(b). And Cloudflare's motion does not even bother to explain the basis for its denial, nor does it provide any information about its investigation, if any. *See* Fed. R. Civ. P. 11(b)(4).

Second, Cloudflare contends that the "FAC falsely alleges" that "when the Argo Tunnel was in place, 'all public traffic accessing Thothub was directed through Cloudflare,'" and "'users could not access Thothub except through Cloudflare.'" (Mot. at 4). Cloudflare again simply asserts that these allegations are "based on the false premise that Cloudflare provided Argo Tunnel services to thothub.tv," without providing any substantiation or support for its assertions. (*Id.* at 5). Notably, Cloudflare does *not* dispute that the FAC's allegations accurately describe the Argo Tunnel. Nor could it. Cloudflare's own website explains that the Argo Tunnel "ensur[es] all requests to [its customer's] resources pass through Cloudflare's security filters" and thereby allows customers to block users that "discover those destinations" (*i.e.*, the IP address of its customer's "origin servers") which would otherwise "provide them with a path around Cloudflare security." (Ex. 2B at App. 30). As Plaintiffs allege, the Argo Tunnel prevents such direct user access.

Third, Cloudflare contends that the "FAC falsely alleges" that, "'if Cloudflare had 'closed' the Thothub tunnel (and ceased delivering Thothub content that Cloudflare had already stored on its servers), as a practical matter, Thothub would no longer have been available on the Internet." (Mot. at 4–5). Cloudflare derides this allegation as "likewise false, and also both speculative and

implausible." (*Id.* at 5). True to form, it offers no supporting evidence. Furthermore, its own statements belie this argument. Cloudflare's website states that, when enabled, the Argo Tunnel ensures that its customers "don't expose an external IP from [their] infrastructure to the Internet." (Ex. 2B at App. 30). And its own briefs in this case contend that Cloudflare's services prevent attacks that can "overwhelm the website, take the victim server offline, and render the site inaccessible." (Dkt 84 at 5–6, quoting *Raisley v. U.S.*, 2016 WL 1117944, *1 (D.N.J. Mar. 22, 2016); *see also* Dkt 84 at 10 n.7, discussing a former Cloudflare customer "whose website was temporarily knocked offline after the withdrawal of Cloudflare's services").

As this record shows, the Argo Tunnel allegations are supported by sufficient evidence to defeat even a motion for summary judgment, much less a Rule 11 motion. Conversely, given the dearth of evidence offered in support of the Rule 11 motion, Cloudflare's motion is frivolous under Rule 11(b)(2) and –(b)(3). Under similar circumstances, a federal court in Florida sanctioned defendants for bringing a frivolous Rule 11 motion. *See Claudet v. First Fed. Cred. Control, Inc.*, 2015 WL 7984410 (M.D. Fla. Nov. 17, 2015). In that case, as here, "[p]erhaps the most startling aspect of Defendant's motion [was] the unsupported premise that defense counsel's proclamation of factual contentions was the coup de grâce," backed only by "Defendant's conclusory answers to Plaintiff's interrogatories." *Id.* at *2 & n.3. "Under Defendant's theory, a reasonably competent attorney would have discharged his or her client's case based solely upon opposing counsel's statements regarding discrete factual issues." *Id.* As in *Claudet*, Cloudflare's view would transform Rule 11 into a hammer for threatening sanctions and obtaining information outside discovery on the sole basis that the defendant denies facts. Even setting aside the ample evidentiary support that exists for the Argo Tunnel

allegations, no reasonable attorney could believe in good faith that this record plausibly supports the imposition of extraordinary Rule 11 sanctions against Plaintiffs based on limited, discrete, highly technical factual allegations in a broad, well-pled complaint.

Moreover, to prevail on the Motion, Cloudflare also must show that Plaintiffs' counsel failed to conduct a reasonable and competent inquiry regarding the allegations. Here, again, Cloudflare's motion falls so far short of the mark as to be frivolous. Indeed, the motion offers no evidence whatsoever regarding Plaintiffs' investigation, relying instead solely on the fact that Plaintiffs' counsel refused to reveal the fruits of its investigation in response to Cloudflare's sanctions threat. (Mot. at 12). Cloudflare's counsel blindly imputes wrongful motives to Plaintiffs' counsel, calling into question opposing counsel's integrity without evidence or basis. *See generally* C.D. Cal. Civility and Professionalism Guidelines.[6] Cloudflare has not served a single discovery request to determine what discoverable information Plaintiffs have, and it cites no authority that would require Plaintiffs to disclose information obtained during its prefiling investigation outside the bounds of discovery simply because Cloudflare denies the allegations.

These issues are especially salient here, where the basis for the allegations includes privileged communications with an employee of Plaintiffs' counsel's client and consulting expert. Cloudflare casts aspersions on Plaintiffs' counsel's representation that the allegations were based in part on privileged "discussions with technical experts." (Mot. at 13). But Rule 11 "does not require a party or an attorney to disclose privileged communications or work product in order to show that the signing of the pleading … is substantially justified." 1983 Cmte. Notes. And as the advisory committee notes make crystal clear, Rule 11 "should not be

[6] Available at: https://www.cacd.uscourts.gov/attorneys/admissions/civility-and-professionalism-guidelines#Preamble (last accessed Jan. 7, 2021).

employed as a discovery device … or to seek disclosure of matters otherwise protected by the attorney-client privilege or the work-product doctrine." 1993 Cmte. Notes. Yet Cloudflare's errant notion that Plaintiffs were duty-bound to disclose such information at Cloudflare's demand is the crux of its motion for sanctions.

Although Cloudflare's motion contains a lengthy legal standards section, it contains little to no application of these rules to the facts here. But comparing this case to those in which sanctions were imposed illustrates the wide gulf between the governing standard and Cloudflare's motion. For example, in *Christian v. Mattel, Inc.*, 286 F.3d 1118 (9th Cir. 2002), the court imposed sanctions based on a voluminous record of misconduct by plaintiff's counsel. For instance, the court found that plaintiff's counsel knew that defendant's allegedly infringing work was created *years before* the date of plaintiff's allegedly infringed work, and that, "[i]n the face of facts and law clearly against his client, [counsel] sought to resurrect the copyright claim by deluging the district court with supplemental filings." *Id.* at 1128–29. Moreover, the court found that counsel's investigation was inadequate because, as he conceded, "he would have been able to discover the copyright information simply by examining the [defendant's accused product]." *Id.* at 1129. The court also noted that the "laundry list of [counsel's] outlandish conduct [was] a long one." *Id.* at 1130–31; *see also Lee*, 468 F. Supp. 3d at 1232 (granting sanctions where the Court found "it completely unreasonable to file a suit premised on an issue debated and analyzed in more than five federal district courts over the last decade"). Cloudflare's motion offers nothing remotely approaching this evidence, nor could it in light of the facts surrounding the Argo Tunnel allegations, Plaintiffs' diligent investigation, and Plaintiffs' counsel's unblemished professional record.

Cloudflare's motion reflects all the infirmities (and more) that it accuses Plaintiffs' complaint of having, made all the worse by the vastly divergent standards of proof required of a complaint versus a Rule 11 motion. *See Sussman v. Bank of Israel*, 56 F.3d 450, 457 (2d Cir. 1995) ("in order to warrant an award of Rule 11 sanctions on the basis that a complaint is not well grounded in fact or law, it must be patently clear that a claim has absolutely no chance of success") (quotation omitted); *E. Gluck Corp. v. Rothenhaus*, 252 F.R.D. 175, 179 (S.D.N.Y. 2008) ("with regard to factual contentions, sanctions may not be imposed unless a particular allegation is utterly lacking in support") (quotation omitted). It makes scurrilous assertions that have no evidentiary basis and are contradicted by evidence. It offers no evidence, even as Cloudflare withholds evidence bearing on the matter. It bespeaks a complete lack of diligence and a "shoot first, aim later" approach to litigation. It makes almost no effort to apply the relevant legal standards to the facts at hand. In short, the Motion is legally and factually baseless, and constitutes an abuse of Rule 11.

II. Cloudflare's Rule 11 Motion Reflects Improper Purposes.

The frivolity of the Motion alone is sufficient to find that Cloudflare should be sanctioned. *See Walker*, at 4 (explaining that, for filings other than a complaint, "a district court may impose Rule 11 sanctions if a paper filed with the court is for an improper purpose, *or* if it is frivolous") (emphasis added and quotation omitted). But the circumstances here make clear that Cloudflare's tactical use of Rule 11 also reveals improper purposes that further justify appropriate sanctions against Cloudflare and its counsel sufficient to deter such abuses in the future.

"Rule 11 is not a toy. A lawyer who transgresses the rule abuses the special role our legal system has entrusted to him." *Draper and Kramer, Inc. v. Baskin-Robbins, Inc.*, 690 F. Supp. 728, 732 (N.D. Ill. 1998). The rule expressly states that

the filer warrants that a motion is "not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation." Fed. R. Civ. P. 11(b)(1). And as noted above, Rule 11 "should not be employed as a discovery device or to test the legal sufficiency or efficacy of allegations in the pleadings … [n]or should Rule 11 motions be prepared to emphasize the merits of a party's position, to exact an unjust settlement, to intimidate an adversary into withdrawing contentions that are fairly debatable, to increase the costs of litigation, … or to seek disclosure of matters otherwise protected by the attorney-client privilege or the work-product doctrine." 1993 Cmte. Notes. Cloudflare's motion here exhibits several such improper purposes.

A. Improper Use as a Discovery Device.—The Motion itself and the Rule 11 letter that preceded it leave little doubt that Cloudflare has improperly used the threat of Rule 11 sanctions as a weapon for discovery. As noted above, although discovery in this case has been open since October 14, 2020, Cloudflare has not served a single discovery request—no requests for production, no fact or contention interrogatories, no deposition requests, *nothing*. Rather than using legitimate discovery processes to ascertain the basis for Plaintiffs' well-founded allegations, Cloudflare sent a threat letter demanding that Plaintiffs "explain the basis for the purported reasonable basis [*sic*] for [Plaintiffs'] belief." (Dkt 102-4 at 4). The Motion doubles-down by arguing that Cloudflare should not have to "shoulder the burden to investigate and disprove *Plaintiffs'* allegations" (Mot. at 13), a tacit admission that Cloudflare has not investigated or disproved the allegations at all. This is not how information is supposed to be exchanged in federal litigation. Cloudflare's circumvention of the rules of discovery is improper, and conduct such as Cloudflare's should be robustly deterred lest more powerful

and better-resourced parties like Cloudflare and its counsel will continue to engage in such tactics strategically in order to gain unfair advantages in litigation.

B. Improper Use to Test Allegations.—Given that Cloudflare fails to present any evidence in support of its denials of the Argo Tunnel allegations and the futility of its sanctions motion, it appears that one purpose of Cloudflare's motion was to probe Plaintiffs' proof and intended use of the Argo Tunnel allegations. But that is not a proper purpose for a Rule 11 motion. The proper vehicle for testing the sufficiency of allegations is through a motion for summary judgment after fulsome discovery or at trial. Cloudflare cannot skip the aspects of litigation that it desperately seeks to avoid—complying with discovery, producing damaging evidence regarding its conduct with respect to Thothub, and airing that evidence in a public forum—by forcing Plaintiffs to litigate these issues on an under-developed, one-sided record. Cloudflare's use of Rule 11 to argue disputed facts is improper. *Cf. Walker*, at 7 (denying Rule 11 motion and sanctioning movant where the purported basis for sanctions turned on matters that were "clearly issues of fact").

C. Improper Use to Emphasize Merits Positions.—One of the most peculiar aspects of Cloudflare's motion is the entirely speculative claim that the "only conceivable purpose of [the Argo Tunnel] allegations is to shore up Plaintiffs' contributory infringement claim, and thereby evade a motion to dismiss, by presenting a fabricated basis on which to argue that Cloudflare should be held contributorily liable for the alleged infringement on Thothub." (Mot. at 5). Not only does this argument ascribe motives to Plaintiffs' counsel that have no basis in fact or evidence, Cloudflare seems to be trying to shape the Court's view of the merits of Plaintiffs' contributory-infringement claims and its pending motion to dismiss, irrespective of what Plaintiffs have alleged and argued in the case.

In fact, the Argo Tunnel allegations represent just a sliver of Plaintiffs' case, and certainly not a linchpin. As explained in Plaintiffs' response to Cloudflare's motion to dismiss (Dkt 93 at 24–25), while the allegations are relevant to disprove Cloudflare's purported factual defense that infringement on Thothub would have continued even without Cloudflare's services, that factual dispute is not central at the motion-to-dismiss stage because, as this Court previously held in rejecting precisely the same argument from Cloudflare, under well-established Ninth Circuit law, a "defendant may still be liable for material contribution regardless of whether it is able to completely halt infringing activity." *ALS Scan, Inc. v. Cloudflare, Inc.*, No. 2:16-cv-05051, Dkt 60, at 7 n.5 (C.D. Cal. Oct. 24, 2016) (citing *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007)). As in *Claudet*, Cloudflare's motion makes scant "reference to the substantive law" and fails to "discuss relevant caselaw." 2015 WL 7984410, at *3. Instead, it improperly uses the Rule 11 motion to advance its misplaced view of copyright law.

D. Improper Use to Intimidate an Adversary.—Cloudflare is a multi-billion-dollar, publicly traded company represented by one of the largest and most powerful law firms in the country, who (based on pleadings and correspondence on this case) has staffed this case with at least three partners and several other attorneys undoubtedly billing at top-of-the-market rates. Plaintiffs are two individuals and a closely-held LLC owned by a third individual, represented by two small (though, we submit, highly capable) law firms working on a contingency basis. Cloudflare's motion unmistakably raises the spectre that Plaintiffs or their counsel may find themselves having to pay Winston and Strawn's legal fees if they do not withdraw the Argo Tunnel allegations, even though those allegations clearly are (at minimum) "fairly debatable." *See* 1993 Cmte. Notes. Indeed, Cloudflare's initial Rule 11 letter says as much, threatening that Cloudflare will seek "an award

of attorney's fees and costs" for the Motion. (Dkt 102-4 at 2). These demands, along with the sheer frivolity of the Motion, suggest an improper purpose to intimidate.

E. Improper Use to Increase the Costs of Litigation.—Along the same lines, as the length of this response brief attests, Cloudflare's baseless motion has forced the Plaintiffs' counsel to expend significant time and resources in order to defend their professional integrity before the Court. *Cf. Claudet*, 2015 WL 7984410, at *3 (finding an improper purpose for a Rule 11 motion in part because the motion "garnered a sixteen-page response from Plaintiff and was likely the source of much anxiety"). Responding to the Motion has not only increased Plaintiffs' costs but also distracted them from pursuing other imperatives in the case, such as moving to compel responses to Plaintiffs' unanswered discovery requests. Not coincidentally, the Motion was filed on December 29 and set for hearing on January 28, forcing Plaintiffs' response brief to be due on January 7, the same week that Plaintiffs previously informed Cloudflare (as a courtesy) they intended to serve a copy of Plaintiffs' portion of the motion to compel in accordance with the local rules. (Ex. 2 ¶ 17). Cloudflare's improper use of Rule 11 is driving up litigation costs for Plaintiffs and delaying other progress in the case.

F. Improper Use to Seek Disclosure of Protected Information.—Finally, Cloudflare's motion reflects an improper attempt to obtain disclosure of privileged communications and work product. When Cloudflare initially accused Plaintiffs (without any supporting evidence, as noted above) of making false allegations with respect to the Argo Tunnel and demanded that Plaintiffs provide the basis for these allegations, Plaintiffs' counsel informed them that part of the basis consisted of privileged communications. Plaintiffs' counsel's communications with Mr. Bell, a consulting expert and employee of Plaintiff Ryuu

Lavitz LLC, are privileged. *See Res. Constructors, LLC v. Ace Prop. & Cas. Ins. Co.*, 2006 WL 3149362, *13 (D. Nev. Nov. 1, 2006) (collecting cases regarding application of the attorney-client privilege to expert consultants).

By filing the Motion, Cloudflare forced Plaintiffs to divulge information and strategy that Cloudflare could not have obtained through legitimate discovery. This benefit alone promises to make the Motion a strategic success and worthwhile endeavor for Cloudflare, at Plaintiffs' and the Court's expense, even if the Court denies the Motion and sanctions Cloudflare and its counsel. The use of Rule 11 to obtain such unfair advantages is improper, and parties like Cloudflare should be justly deterred from doing such things in the future.

CONCLUSION

The Motion should be denied. Because the Motion was frivolous and brought for an improper purpose, the Court should appropriately sanction Cloudflare and its counsel, including by awarding costs and expenses under Rule 11(c)(2). In addition, the Court should consider imposing additional penalties—including punitive monetary sanctions and remedial ethics courses—in order to deter future misconduct, taking into account Cloudflare's and its counsels' financial status.

Respectfully submitted,

By: Brett S. Rosenthal

REESE MARKETOS LLP
Brett S. Rosenthal (*pro hac vice*)
Joshua M. Russ (*pro hac vice*)
Sean F. Gallagher (*pro hac vice*)
Joel W. Reese (*pro hac vice*)
750 N. Saint Paul Street, Ste. 600
Dallas, Texas 75201-3202
Telephone: (214) 382-9810
Brett.rosenthal@rm-firm.com

REITER GRUBER LLP
Charles Reiter (SBN 306381)
Robert Gruber (SBN 301620)
100 Wilshire Blvd, Suite 700
Santa Monica, California 90401-3602
Telephone: (310) 496-7799
creiter@reitergruber.com

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that the above document will be served at the time of filing on all counsel of record via the Court's electronic filing system.

/s/

Brett S. Rosenthal