Robert B. Owens, Esq. (Bar No. 77671)
rowens@ogrlaw.com
OWENS & GACH RAY
10323 Santa Monica Blvd., Suite #102
Los Angeles, CA 90025
Ph: (310) 553-6611
Fax: (310) 954-9191

Craig S. Hilliard, Esq.
chilliard@stark-stark.com
Gene Markin, Esq.
gmarkin@stark-stark.com
STARK & STARK, P.C.
993 Lenox Drive, Bldg. Two
Lawrenceville, NJ 08648
Ph: (609) 895-7248
Fax: (609) 895-7395
(*Pro Hac Vice* Applications Granted)

Attorneys for Plaintiffs
Mon Cheri Bridals, LLC and
Maggie Sottero Designs, LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

(SAN FRANCISCO DIVISION)

MON CHERI BRIDALS, LLC and MAGGIE SOTTERO DESIGNS, LLC, Plaintiffs, **vs.** **CLOUDFLARE, INC**., a Delaware corporation; and DOES 1-10, Inclusive, Defendants.	Case No. 19-CV-01356-VC **PLAINTIFFS' REPLY BRIEF IN FURTHER SUPPORT OF MOTION FOR SUMMARY JUDGMENT AND OPPOSITION TO CLOUDFLARE'S CROSS-MOTION FOR SUMMARY JUDGMENT**

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

CITATION GUIDE

Declarations

- "**Petrossian Decl**." refers to the Declaration of Armen Petrossian.
- "**Photographer Declarations**" refers to the Declarations of Danny Cardozo, Rich McMullin, and Adam Flipp.

Depositions

- "**Paine Dep 3**" refers to Deposition Transcript of Justin Paine dated April 30, 2021.
- "**Jonyer Dep**" refers to Deposition Transcript of Istvan Jonyer, Ph.D dated April 29, 2021.

Other References

- "**Exh**." refers to an Exhibit attached to either the Declaration of Gene Markin or the Supplemental Declaration of Gene Markin unless otherwise noted.
- "**Jonyer Rebuttal Report**" refers to the Rebuttal Expert Report of Istvan Jonyer, Ph.D dated August 19, 2020.
- "**PSF**" refers to Plaintiffs' Statement of Undisputed Facts in support of motion for summary judgment.

SUMMARY OF RESPONSE

Playing the victim, Cloudflare paints itself as an internet security service provider with no ability to control infringement by its users or to eliminate infringing material from the Internet. But that is not the standard. Just because a book publisher cannot stop an author from making and selling additional copies of an infringing work does not mean the publisher is not liable for publishing infringing works after being notified of the infringement. The same is true here – try as it may to hide under the guise of helplessness, Cloudflare most certainly has several simple non-onerous tools at its disposal to curb infringement such as removing infringing content from its cache servers, ceasing caching services, and preventing access to infringing webpages – all of which can be done with a few clicks of a mouse.

Sure, users can stop using Cloudflare and continue infringing, but it would not be as effective and damaging to copyright owners without the benefit of Cloudflare's services (domestic storing and serving of images, faster load times, higher conversion rates). The law does not require Cloudflare to control the actions of others, but only to do what it reasonably can and should do to prevent continued infringement *using its services* after notice.

Alas, merely forwarding an infringement complaint to an email address, which may or may not be monitored, does not suffice when Cloudflare receives consecutive infringement complaints concerning the same domain client. Far from "faulty," Plaintiffs' notifications of claimed infringement contain all the specific information needed for Cloudflare to confirm the infringement and to take action. Regardless of how the notifications were titled or what section of the DMCA they reference, the content gave Cloudflare specific information about the infringement, *i.e.* name of copyright owner, URL link to original copyrighted image, name of infringing domain, URL of infringing page and location of infringing image, and a request that Cloudflare remove the infringing content from its servers and disable access to the infringing

content. Turning a blind eye, Cloudflare continued providing services, which were used by the infringers to bait and switch American consumers.

Cloudflare downplays the benefits of its optimization and web performance services for purposes of legal argument, but prides itself on the exceptional speed and optimization advantages its services provide when trying to attract customers. In our fast-paced technology driven world, milliseconds make a difference, and by Cloudflare's own admission speed matters when it comes to user engagement and online sale conversions. And that's why infringers flock to Cloudflare – to get quick, reliable, and secure access to American online consumers who are duped into purchasing knockoff dresses using Plaintiffs' hard-earned images.

Finally, not only has Cloudflare failed to implement a reasonable repeat infringer policy, but given the breadth and interrelatedness of Cloudflare's services, Cloudflare does not qualify for either of the DMCA safe harbors it attempts to invoke. Consequently, Cloudflare's cross-motion for summary judgment must be denied and Plaintiffs' motion granted.

SUPPLEMENTAL FACTS

Cloudflare's Repeat Infringer Policy

Members of Cloudflare's Trust & Safety team manually review infringement complaints submitted to Cloudflare for completeness – and if incomplete, Cloudflare responds to the reporter requesting the missing or incomplete information. Paine Dep 1 (Exh. N), 42:10 to 45:15, 51:10 to 52:24, 250:3 to 252:25. When Cloudflare gains a certain comfort level with a reporter based on consistency of complete abuse reports, [redacted]. *Id.*, 45:16 to 49:7.

At some point, Counterfeit Technology was added to Cloudflare's [redacted] which means Cloudflare automatically responded to Counterfeit Technology with the name of the

hosting provider as well as notified the hosting provider and its customer of the infringement complaint. *Id.*, 49:13 to 51:9, 56:21 to 64:8. Cloudflare, however, does not expect and oftentimes does not receive a response back from its customer to such notices. *Id.*, 67:3 to 71:9.

Cloudflare has the ability to investigate the claims of infringement by clicking on the links provided by Counterfeit Technology to compare the original image with the alleged infringing image, but does not, citing "security" concerns (even though Cloudflare, an Internet security company, has systems in place to detect malicious links or spyware). *Id.*, 244:3 to 245:25.

Between 2011 and December 2019, [redacted]. *Id.*, 73:16 to 76:15. Prior to December 2019, [redacted]. *Id.*, 76:3 to 77:6, 285:12 to 286:20.

[redacted], Cloudflare – for the first time – put its "repeat infringer policy" in writing. *See* Cloudflare's Written Repeat Infringer Policies (Exh. QQ). At the time, [redacted]. *Id.* [redacted], Cloudflare adopted a written step-by-step process for identifying potential repeat infringers, evaluating prospective repeat infringers, and terminating services to those websites found to be repeat infringers. *Id.* at CLOUDFLARE-MCB00010926-28; Paine Dep 2 (Exh. PP), 79:4-14.

In a nutshell, [redacted]

[redacted]. Paine Dep 1, 81:1 to 106:21, 118:14 to 125:21. [redacted]. *Id.*, 135:6 to 137:5.

[redacted]. Paine Dep 3 (Exh. RR), 5:2 to 6:10. [redacted]. *Id.*, 15:3 to 16:4. [redacted]. *Id.*, 51:20 to 55:15.

[redacted]. *Id.*, 23:20 to 26:15 [redacted]

[redacted] *Id.*, 26:16-24. [redacted] . *Id.*, 26:19 to 27:7.

Even though Paine initially testified that prior to December 2019, Cloudflare had not terminated services to domains solely as a result of infringement complaints, Cloudflare later produced a spreadsheet containing a list of domain clients that were purportedly terminated [redacted] . Paine Dep 1, 138:2 to 139:1; Spreadsheet of Terminated Domains (Exh. UU). [redacted] . Paine Dep 3, 98:13 to 101:14. [redacted] . *Id.*, 101:15 to 103:9.

[redacted] . Paine Dep 2 at 61:22 to 65:4. [redacted] . *Id.*, 136:8-14.

Additionally, Cloudflare's repeat infringer policy focuses on [redacted]

[redacted]. Paine Dep 1, 293:3 to 296:24; Paine Dep 3, 41:25 to 42:19. Thus, [redacted]. *Id.,* 303:19 to 307:11.

And even when Cloudflare deems a domain to be a repeat infringer under its policy [redacted]. *Id.*, 314:6 to 319:1; Paine Dep 2, 83:20 to 84:8. Moreover, Cloudflare does not consistently and uniformly apply its revamped infringer policy: [redacted]. Paine Dep 3, 56:1 to 66:9; Repeat Infringer Reports for July-December 2019 (Exh. SS). And in 2020, [redacted]. Paine Dep 3, 66:10 to 75:16; Repeat Infringer Reports for February-May 2020 (Exh. TT).

With respect to disciplinary actions, [redacted]. Paine Dep 3, 75:17 to 80:6.

LEGAL ARGUMENT

I. CLOUDFLARE IS LIABLE FOR CONTRIBUTORY INFRINGEMENT

Based on a distorted, selective reading of the applicable case law, Cloudflare seeks to require Plaintiffs to prove "active, culpable intent;" however, the requisite intent is imputed when a defendant knowingly continues to contribute to infringing behavior. *Amazon*, 508 F.3d at 1172[1]. According to the Ninth Circuit, culpable intent is imputed when a defendant "has actual knowledge that specific infringing material is available using its system," is able to "take simple measures to prevent further damage to copyrighted works," yet continues "to provide access to infringing works." *Id*. Thus, intent is imputed from the defendant's failure to take "reasonable and feasible steps" in the face of specific knowledge. *Id.*

A. Cloudflare Substantially Assists Infringement

"Material contribution turns on whether the activity in question 'substantially assists' direct infringement." *Louis Vuitton Malletier, S.A. v. Akanoc Sols., Inc*., 658 F.3d 936, 943 (9th Cir. 2011) (citation omitted). Since providing direct infringers with server space satisfies that standard, so too does Cloudflare's continued caching of infringing images. *Id*.; *see also ALS SJ*[2] *at p. 16* (Exh. CCC) (finding plaintiff can establish Cloudflare "substantially assisted" infringement by creating cache copies through its CDN Network).

Cloudflare claims its services do not "significantly magnify the effects of otherwise immaterial infringing activities." But the Ninth Circuit emphasized that "services or products that facilitate access to [infringing] websites throughout the world can significantly magnify the effects of otherwise immaterial infringing activities." *Amazon*, 508 F.3d at 1172 (internal quotations and citations omitted). That is exactly what Cloudflare does. By its own admission

[1] *Perfect 10, Inc. v. Amazon.com, Inc*., 508 F.3d 1146 (9th Cir. 2007) ("*Amazon*").
[2] *ALS Scan, Inc. v. Cloudflare, Inc., et al*., Case No. 2:16-cv-5051 (C.D. Cal. Mar. 13, 2018) ("*ALS SJ*")

and value proposition, websites hosted overseas will load faster, work better, and be more secure with the help of Cloudflare. PSF, ¶¶ 17-35, 39-43.

And while Cloudflare likens itself to the credit card companies in *Visa*[3] where the payment processors were found to not materially assist the infringement because no "infringing material passes over [d]efendants' payment networks or through their payment processing systems" and there was no allegation that "[d]efendants' systems are used to alter or display the infringing images," Cloudflare's services do all those things. 494 F.3d at 795. At a browser's request, Cloudflare will fetch and then use its network and tools to deliver infringing content, either from the host or its own cache servers, in a fast, reliable, and efficient manner – and in fact, Cloudflare's network is the *only* way for the general public to access the infringing material.[4]

Accordingly, there can be no doubt Cloudflare's services materially assist the infringers.

B. Simple Steps Cloudflare Can Take

Relying on *ALS Scan*[5], Cloudflare argues its forwarding of infringement complaints to hosts and clients suffices to absolve Cloudflare of any secondary liability. Significant to the Ninth Circuit's holding that defendant's simple measures were enough is that after notice was sent "every infringing work was taken down." 819 F. App'x at 524. There was nothing more ALS Scan could do to prevent further infringement. *Id.* ("What measures were available to prevent further damage to ALS's copyrighted images, Steadfast took.").

Not the same here. Cloudflare's notices to hosting providers and clients are wholly ineffective. In the case of the 174 Repeat Infringer Domains, each one continued to use Plaintiffs' images even after Cloudflare's notice. In fact, Plaintiffs continued to submit notices

[3] *Perfect 10, Inc. v. Visa Int'l Serv., Ass'n*, 494 F.3d 788 (9th Cir. 2007) ("*Visa*")
[4] When Cloudflare's required and recommended settings are enabled, which is more often than not the case. PSF, ¶¶ 36-38.

to Cloudflare about the same domains using the same images but Cloudflare took no meaningful steps to curb the infringement. *See* Petrossian Decl.[6], ¶¶ 2-5; Repeat Notice Spreadsheet, Exh. 1 to Petrossian Decl.

It is reasonable to require Cloudflare do more after receiving notice of specific infringements by specific domains. It can easily remove infringing content from its cache, cease providing caching services, and block access through its network to infringing content. PSF, ¶¶ 63-71; Paine Dep 3, 75:17 to 80:6; *see Giganews*, 847 F.3d at 671[7] (to be considered "simple measures," the measures must be not "onerous" or "unreasonably complicated").

It matters not that infringers *could* stop using Cloudflare's services and continue infringing without Cloudflare's help. What matters is that Cloudflare can foreclose the use of its network and website optimization and performance tools to aid infringement but chooses not to. *See ALS SJ* at p. 18 ("The simple answer as to whether Cloudflare could have done something simple to stop the infringement is "yes": Cloudflare can, but does not, end its business relationship with websites that it knows (or arguably knows) are serial infringers … While Cloudflare may do amazing things for internet security, the Court would have a hard time accepting that Cloudflare's security features give it license to assist in *any* online activity.").

C. Specific Knowledge of Infringement

The Ninth Circuit interprets the knowledge requirement for contributory copyright infringement to include both those with *actual knowledge* and those who have *reason to know* of direct infringement. *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004). There is no requirement that Plaintiffs' infringement notices comply with Section 512(b)(2)(E)(ii) to confer actual knowledge on Cloudflare. Here, Plaintiffs' notices gave Cloudflare specific information

[5] *ALS Scan, Inc. v. Steadfast Networks, LLC*, 819 F. App'x 522, 523 (9th Cir. 2020) ("*ALS Scan*")
[6] The Declaration of Armen Petrossian in Further Support of Plaintiffs' Motion for Summary Judgment and In Opposition to Cloudflare's Cross-Motion for Summary Judgment (the "Petrossian Decl.").

about the copyright owner, the copyrighted image, the infringing domain, the location of the infringing material, and all the information Cloudflare needed to confirm its domain clients were using Plaintiffs' images. *See Giganews 2014*[8], at *23 (a DMCA notice that identifies "the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material" confers actual knowledge on the recipient).

Cloudflare spends considerable time attacking Counterfeit Technology's competency, technology, and proofs submitted in other unrelated cases. But none of that matters because at the end of the day a human being – not a computer – confirmed that an allegedly infringing image matched the original image before sending notice to Cloudflare. PSF, ¶ 50. And that information along with the specific infringing URL and domain name were provided to Cloudflare and conferred specific knowledge regardless of the DMCA section that was cited. And while the notices may not have triggered a duty to act under Section 512(b), they nevertheless required Cloudflare take simple, reasonable steps to prevent further infringement using its services.

Finally, the potential for false or bad-faith infringement notices is not reason enough to not act on infringement complaints – especially when the senders, copyright owners, works, and potential infringement can be verified (by clicking the links provided). The existence of bad actors who submit false infringement accusations for improper purposes should not overshadow and hinder the rights of copyright owners with legitimate infringement concerns. By continuing to provide cache server space and website optimization and security services to websites

[7] *Perfect 10, Inc. v. Giganews, Inc*., 847 F.3d 657, 671 (9th Cir. 2017) ("*Giganews*").
[8] *Perfect 10, Inc. v. Giganews, Inc*., No. CV 11-07098-AB (SHx), 2014 U.S. Dist. LEXIS 183590 (C.D. Cal. Nov. 14, 2014) ("*Giganews 2014*").

continuously accused of infringement, Cloudflare is not making the Internet a "safer" place but rather making Cloudflare a "safe haven" for infringers.

II. PLAINTIFFS' OWNERSHIP OF COPYRIGHTS & PROVING UNDERLYING INFRINGEMENT

A. Plaintiffs Own Valid Copyrights in the Works

Cloudflare argues Plaintiffs cannot show ownership in the infringed photographic works. *First*, there is no dispute between the photographers and Plaintiffs regarding ownership and Cloudflare has not adduced any evidence or testimony showing anyone contests Plaintiffs' ownership. Accordingly, when there is no dispute between the copyright owner and contractor/transferee, "it would be unusual and unwarranted to permit a third-party infringer to invoke [§ 101 or § 204(a)] to avoid suit for copyright infringement." *Jules Jordan Video, Inc. v. 144942 Canada Inc*., 617 F.3d 1146, 1157 (9th Cir. 2010) (internal citations omitted).

Second, the work-for-hire agreements between Plaintiffs and their photographers are signed by photographers who agreed to take photos on a work-for-hire basis and agreed to *transfer and assign any ownership in the photographs to Plaintiffs*. This satisfies the requirements of Section 204(a) dealing with assignments, which Cloudflare lacks standing to challenge. *See Magnuson v. Video Yesteryear*, 85 F.3d 1424, 1428 (9th Cir. 1996) (concluding where there is no argument between assignor and assignee, "it would be anomalous to permit a third-party infringer to invoke [the writing requirement] against the licensee").

Third, any inadvertent discrepancies or mistakes in Plaintiffs' certificates, such as indicating authorship via work-for-hire versus assignment, do not automatically invalidate the certificates and their corresponding presumption of ownership. *See Urantia Found. v. Maaherra*, 114 F.3d 955, 963 (9th Cir. 1997) ("inadvertent mistakes on registration certificates do not invalidate a copy-right and thus do not bar infringement actions, unless . . . the claimant

intended to defraud the Copyright Office by making the misstatement"). "Absent intent to defraud and prejudice, inaccuracies in copyright registration do not bar actions for infringement." *Harris v. Emus Records Corp*., 734 F.2d 1329, 1335 (9th Cir. 1984). Cloudflare has not alleged fraud nor does it contend any prejudice results from listing the works as works for hire. *See Testa v. Janssen*, 492 F. Supp. 198, 201 (W.D. Pa. 1980) (false representation of authorship on copyright certificate when ownership was through assignment did not warrant application of unclean hands). As such, the alleged inconsistencies in Plaintiffs' certificates do not rebut the presumption of ownership.

Thus, Plaintiffs' work-for-hire agreements with photographers, valid copyright certificates, deposition testimony, and declarations provide competent evidence of copyright ownership predating the infringement. *See* Declarations of Photographers; PSF, ¶¶ 1-7; Examples of Notices to Cloudflare re Infringement of Images Registered Prior to Discovery of Infringement (Exh. DDD).

B. Plaintiffs Are Not Seeking Relief Against Doe Defendants

Cloudflare incorrectly posits that Plaintiffs must prosecute fictitious defendants as a threshold requirement for proving underlying infringement giving rise to Cloudflare's contributory liability. The authority Cloudflare cites illustrates that identifying and serving John Does is needed to obtain relief *against* those unnamed defendants.[9]

Here, Plaintiffs are not seeking any relief against the Does, but rather seeking a finding that underlying infringement has occurred for purposes of determining Cloudflare's contributory liability. There is no precedent to require a contributory infringement plaintiff to prosecute Doe

[9] *See, e.g., Reed v. Cox*, 821 F. App'x 836, 837 (9th Cir. 2020) (seeking relief from fictitious defendants for alleged violations of 42 U.S.C. § 1983); *Gillespie v. Civiletti*, 629 F.2d 637, 639 (9th Cir. 1980) (seeking relief from fictitious defendants for alleged violations of plaintiff's constitutional rights); *Chenault v. San Ramon Police Dep't*, No. 15-cv-03662-SK, 2016 U.S. Dist. LEXIS 121632, at *2 (N.D. Cal. Sep. 8, 2016) (seeking relief from fictitious defendants for alleged violations of plaintiff's constitutional rights)

direct infringers. Neither the Supreme Court nor the Ninth Circuit has required plaintiffs to bring an action against end user infringers in contributory infringement cases.[10]

Because Plaintiffs have shown ownership of the works at issue and a violation of their exclusive rights, Plaintiffs need not prosecute Doe defendants for the underlying infringement to succeed on their claim of contributory infringement against Cloudflare. *See Napster*, 239 F.3d at 1013.

III. CLOUDFLARE IS NOT ENTITLED TO DMCA SAFE HARBOR

The DMCA was "enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider." *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001) (internal citations omitted). This immunity is not presumptive, but granted only to "innocent" service providers who can show they do not have a defined level of knowledge regarding the infringement on their system. *Id.* The DMCA's protection disappears "at the moment [the service provider] becomes aware that a third party is using its system to infringe." *Id.*

A. Cloudflare Has Failed to Adopt and Reasonably Implement A Repeat Infringer Policy

To fulfill the requirements of § 512(i)(1)(A), "a service provider must (i) adopt a policy that provides for the termination of service access for repeat infringers; (ii) inform users of the service policy; and (iii) implement the policy in a reasonable manner." *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 744 (S.D.N.Y. 2011). As one court observed, "[t]he purpose of subsection 512(i)

[10] *See, e.g.*, *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930-31 (2005) ("When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement."); *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 434 (1984) (plaintiffs not required to bring action against direct copyright infringers to sustain claim for secondary liability); A*&M Records v. Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001) ("*Napster*") (same); *Visa*, 494 F.3d at 794 (same)

is to deny protection to websites that tolerate users who flagrantly disrespect copyrights." *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 637 (S.D.N.Y. 2011).

Cloudflare's amorphous policy of dealing with potential repeat infringers and the inconsistent implementation of that policy do not satisfy the requirements of the DMCA. While Cloudflare reserves the right to investigate users and their infringement activities and to terminate/suspend services after receiving any number of DMCA complaints, Cloudflare took no such action in response to the thousands of infringement complaints it received from Plaintiffs.[11] Despite repeated infringement notices, Cloudflare did not take any action against any Repeat Infringers except in June 2017 when it terminated services to some domains – seemingly in an attempt to muster compliance with the DMCA – yet continued providing services to the remaining known infringers. *See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007) ("A policy is unreasonable . . . if the service provider failed to respond when it had knowledge of the infringement. . . .").[12] Notably, eight of the allegedly "terminated" infringers continued using Cloudflare's services after June 2017 giving rise to subsequent infringement complaints from Counterfeit Technology. *See* Petrossian Decl., ¶¶ 8-9; Exhs. 3 & 4, Petrossian Decl.

Prior to December 2019, Cloudflare's repeat infringer policy consisted of terminating services to users *only* when ordered to do so by a court; admittedly, Cloudflare has not terminated services to domains *solely* as a result of DMCA complaints regardless of the quantity,

[11] *See* Cloudflare's Terms of Service Agreements (Exhibits VV-ZZ); Paine Dep 2, 40:4-16; *see also* Exh. 1 to Petrossian Decl.

[12] See also *Corbis Corp. v. Amazon.com, Inc.,* 351 F. Supp. 2d 1090, 1104 (W.D. Wash. 2004) ("Even with proper enforcement procedures, a copyright holder may still demonstrate that the service provider has not satisfied § 512(i) if there are specific instances demonstrating that the service provider tolerates repeat copyright infringement by its users."); *Ventura Content, Ltd. v. Motherless, Inc*., 885 F.3d 597, 622 (9th Cir. 2018) (failure to terminate the account of a repeat infringer raised a material issue of fact regarding whether defendant's policy satisfied § 512(i)(1)(A) requirement); *Io Grp., Inc. v. Veoh Networks, Inc*., 586 F. Supp. 2d 1132, 1143 (N.D. Cal. 2008) (implementation of a repeat infringer policy "is reasonable if, under appropriate circumstances, the service provider terminates users who repeatedly or blatantly infringe copyright) (internal citations and quotes omitted).

diversity, and legitimacy of those complaints.[13] S*ee Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1177-78 (C.D. Cal. 2002) (Section 512 does not endorse business practices that "would encourage content providers to turn a blind eye to the source of massive copyright infringement while continuing to knowingly profit, indirectly or not, from every single one of these same sources until a court orders the provider to terminate each individual account").

Additionally, Cloudflare treats each domain separately rather than look at domains owned by the same user collectively.[14] This means that even though Cloudflare may act against an infringing domain, a user can simply add new domains to the account and continue infringing without recourse. In fact, it appears that many of the Repeat Infringers are owned/operated by just a handful of owners. Exh. 2, Petrossian Decl. And while a significant number of complaints against a single domain may trigger that domain's inclusion on a potential repeat infringer list, that same number of complaints spread across all domains owned by the same user will not subject the user or any of the domains to investigation. And so users can easily get around Cloudflare's policy, which is overrun with loopholes and deficiencies making it wholly ineffective in curbing infringement by its users. *See Cybernet Ventures*, 213 F. Supp. 2d at 1177-78 (a service provider fails to properly implement an infringement policy where it fails to terminate a user even though it has sufficient knowledge of that user's blatant, repeat infringement of a willful and commercial nature … the repeat infringer policy requirement should provide "strong incentives" for service providers to prevent their services from becoming safe havens or conduits for known repeat copyright infringers).

Finally, Cloudflare does not uniformly apply its policy: sometimes it will terminate services and sometimes not regardless of how many infringement complaints it receives.[15] And

[13] Paine Dep 1, 73:16 to 77:6, 285:12 to 286:20; Paine Dep 2, 136:8-14.
[14] Paine Dep 1, 293:3 to 296:24, 303:19 to 307:11; Pain Dep 3, 41:25 to 42:19.
[15] Paine Dep 3, 56:1 to 75:16; Repeat Infringer Reports for 2019 & 2020 (Exhs. SS & TT).

even when Cloudflare determines a domain to be a repeat infringer, it only terminates caching services but continues to provide security, DNS, and reverse-proxy services which infringers use to continue infringing.[16]

Despite having the tools and ability to effectively block access to infringing material (until the issue is resolved or the user stops using Cloudflare's services), Cloudflare does not, opting instead to continue storing, serving, and transmitting infringing material.[17] *See In re Aimster Copyright Litig.*, 334 F.3d 643, 654-55 (7th Cir. 2003) (DMCA safe harbors require that the service provider "do what it can reasonably be asked to do to prevent the use of its service by 'repeat infringers'"). Accordingly, Cloudflare's "policy" is a far cry from policies courts have found to comply with § 512(i).[18]

B. Cloudflare Does Not Qualify for Safe Harbor Under Sections 512(a) or 512(b)

A party moving for summary judgment on an affirmative defense, such as a service provider asserting a right to a safe harbor limitation under the DMCA, "must establish beyond controversy every essential element, and failure to do so will render [the service provider] ineligible for the . . . safe harbor's protection." *Mavrix Photographs, LLC v. Livejournal, Inc.*, 873 F.3d 1045, 1052 (9th Cir. 2017) (internal quotes and citations omitted). Most courts have refused to determine whether a party is entitled to protection under the DMCA on a motion for summary judgment, noting that "it is difficult to conclude as a matter of law [that a defendant] ha[s] 'reasonably implemented' a policy against repeat infringers." *ALS Scan v. Cloudflare, Inc.*,

[16] Paine Dep 1, 314:6 to 319:1; Paine Dep 2, 83:20 to 84:8; *see also* Exhs. 3 & 4, Petrossian Decl.
[17] Paine Dep 3, 75:17 to 80:6.
[18] *See, e.g., Hempton v. Pond5, Inc.*, No. 3:15-cv-05696-BJR, 2016 U.S. Dist. LEXIS 147830, at *22-23 (W.D. Wash. Oct. 25, 2016) (defendant satisfied threshold requirements of § 512(i) where it removed challenged content and suspended user after receiving a DMCA take down notice); *Corbis Corp.*, 351 F. Supp. 2d at 1103 (Amazon's practice of promptly canceling a listing after receiving notice of infringement and warning implicated vendors that repeated violations may result in permanent suspension complied with DMCA threshold requirements); *Arista Records LLC v. Myxer Inc.*, No. CV 08-03935 GAF (JCx), 2011 U.S. Dist. LEXIS 109668, at *71 (C.D. Cal. Apr. 1, 2011) (defendant presented evidence of arguably adequate policy where defendant "processes DMCA notices immediately and disables infringing material usually within one business day of the notice").

No. CV 16-5051-GW(AFMx), 2018 U.S. Dist. LEXIS 243750, at *23 (C.D. Cal. Feb. 5, 2018) (citations omitted).

(i) Section 512(a)

The Transitory Communications Safe Harbor requires that: (i) "no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network *in a manner ordinarily accessible to anyone other than anticipated recipients*" and (ii) "no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a *longer period than is reasonably necessary for the transmission, routing, or provision of connections*." § 512(a)(4) (emphasis added).

When a user visits a web page, the content is delivered from the host server (or local cache server) through many small units of data called packets, which travel through a network of routers and switches (the Internet) until they are reassembled at their destination (user's computer). Jonyer Rebuttal Report (Exh. AAA), p. 4; Jonyer Dep (Exh. BBB), 164:16-25. These routers/switches quickly forward packets to the next router/switch; however, "if the speed with which the packets arrive at the switching equipment is faster than the speed with which they leave it, then the switch will have to buffer (store) some packets waiting to be sent out." *Id*. Thus, the time "reasonably necessary for the transmission, routing, or provision of connections" is the time it takes the packets to travel through a series of switches/routers on their way from the origin server to the requesting machine (user's computer). *Id*., p. 5; Jonyer Dep, 112:14 to 113:21.

To wit, the legislative history confirms that 512(a) was meant to "include routing of packets from one point to another on the Internet" and the statute's reference to "intermediate and transient storage" refers to copies of information made by routing equipment "in the course of moving packets of

information across digital on-line networks."[19] Thus, subsection (a)(4) covers "copies made of material while it is en route to its destination".[20]

Since Cloudflare stores a copy of the transmitted material in its cache for much longer than reasonably necessary for the actual transmission of that data to the requester, it does not qualify for the safe harbor. Jonyer Report (Exh. EE), pp. 52-55; Jonyer Rebuttal Report, pp. 3-6; *see, e.g., Columbia Pictures Indus. v. Gary Fung*, 710 F.3d 1020, 1041 (9th Cir. 2013) ("§ 512(a) applies to service provides who act *only* as "conduits" for the transmission of information") (emphasis added); *UMG Recordings, Inc. v. Shelter Capital Partners Ltd. Liab. Co*., 718 F.3d 1006, 1019 n.10 (9th Cir. 2013) (noting that § 512(a) applies where the service provider "merely acts as a conduit for infringing material *without storing, caching*, or providing links to copyrighted material," and thus "*has no ability to remove the infringing material from its system* or disable access to the infringing material") (emphasis added) (internal quotation marks omitted).

Moreover, each transmission contemplated by 512(a) has an intended/anticipated recipient, *i.e.* the requester. Jonyer Dep, 115:25 to 116:14. Subsequent requesters trigger separate transmissions. The statute's use of the plural "anticipated recipients" does not mean subsequent requesters who may be served the same material from cache; rather, it means multiple recipients of the transmission (not subsequent transmissions), such as multicast protocols. *Id*., 103:8 to 104:15. This is supported by the legislative history, which provides that the term "ordinarily accessible" in 512(a)(4) "does not include copies made by a service provider for the purpose of making the material available to other users. Such copying is addressed in subsection (b)." H.R. REP. NO. 105-551, pt. 2, at 51.

As such, Cloudflare does not qualify for the safe harbor because it does not simply transmit and route data through its network but rather stores copies of the material on its cache servers for

[19] See H.R. REP. NO. 105-551, pt. 1, at 24 (1998); *see also id*., pt 2, at 50-51 ("In this context, 'intermediate and transient' refers to such a copy made and/or stored in the course of a transmission, not a copy made or stored at the points where the transmission is initiated or received.")

"longer [] than is reasonably necessary for the transmission, routing, or provision of connections" and such cached material is made available to subsequent requesters of the material, not just the "anticipated recipients" who request the material prior to it being stored in cache. PSF, ¶¶ 19, 23-30, 46; Jonyer Dep, 123:22 to 133:23.

(ii) Section 512(b)

"Section 512(b) applies to a different form of intermediate and temporary storage than is addressed in subsection (a)." H.R. REP. NO. 105-551, pt. 2, at 51. The System Caching Safe Harbor shields a service provider from liability "by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider" provided "*the material is made available online by a person other than the service provider*." § 512(b)(1)(A) (emphasis added).

Because Cloudflare's services are designed to regulate *all* traffic to and from its clients' websites, the *only* way for end users to access those websites is through Cloudflare (when Cloudflare's required and recommended settings are enabled), and therefore, Cloudflare makes its clients' material "available online." Jonyer Report, pp. 55-61; Jonyer Rebuttal Report, pp. 6-8; Jonyer Dep, 140:5 to 141:20, 153:2-19, 158:19 to 160:11. Content is made "available online" when it is publicly accessible through regular means (*i.e.*, typing URL into browser, Google search, etc.); the mere act of putting material on a web server does not make that material publicly available unless there is a means by which the public can access it. Jonyer report, pp. 6-7.

Regardless of which internet provider, hosting service, internet gateway, routing pathway, or equipment is used, a client's website contents are only accessible to the public through Cloudflare's network and only if Cloudflare allows the transmission to proceed. Jonyer Dep, 153:2-19. A request for client content must pass through Cloudflare before reaching the host server or a cache server;

[20] *Id*. at p. 51.

Cloudflare has the ability to restrict public access to content stored anywhere in the world for as long as the client remains a Cloudflare customer and has implemented the recommended settings. Jonyer Dep, 159:16-24, 187:1 to 191:24. Cloudflare is therefore the gatekeeper of public access to online material and has a master switch to turn off or enable access to that material. Jonyer Report, pp. 56-58.

As such, Cloudflare does not meet the requirements of the safe harbor because when Cloudflare's default CDN, caching, reverse-proxy, and DNS settings are enabled (which is the standard setting used by the majority of domain clients), any and all of Cloudflare's clients' website content and material is made available online by Cloudflare – not "a person other than the service provider [i.e., Cloudflare]". PSF, ¶¶ 31-38, 70.

Moreover, this safe harbor does not apply where, as here, contributory liability is also premised on Cloudflare's material contribution to the infringing activities of its clients by continuing to provide non-caching related website security, optimization, DNS, and reverse-proxy services after receiving notice of the infringing activities (such as continuing to securely and optimally serve infringing material from origin servers). *See In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 660-61 (N.D. Ill. 2002) (finding Section 512(b) inapplicable where liability arises from non-caching activities).

CONCLUSION

For all the foregoing reasons, Plaintiffs' Motion for Summary Judgment must be granted and Defendant Cloudflare's Motion for Summary Judgment must be denied.

RESPONSES TO CLOUDFLARE'S OBJECTIONS TO EVIDENCE

A. Entire Transcript Exhibits. Plaintiffs have attached the entire transcripts of depositions in order to have a complete record and to be able to cite to different portions in their opposition without having to attach disjointed portions of the transcripts.

B. Lay Witness Declarations. The Declarations of Jon Liney, Hilary Taylor, and Suren Ter-Saakov, and the exhibits thereto, are based on the declarants' personal knowledge and evidence in the record. Each declarant was fully deposed by Cloudflare who had the opportunity to cross-examine them on the topics contained in their declarations, the data and information underlying the exhibits referenced in their declarations, and all the exhibits marked at depositions. Ter-Saakov's use of the word "we" does not obscure or negate his personal knowledge and involvement in the work and processes involved in preparing the referenced exhibits, which are all based on data, documents, and evidence produced in discovery.

Respectfully submitted,

By: /s/ *Gene Markin*

GENE MARKIN, ESQ.
STARK & STARK, P.C.
993 Lenox Drive
Lawrenceville, NJ 08648
(609) 895-7248

Attorneys for Plaintiffs

Dated: July 28, 2021