ANDREW P. BRIDGES (CSB No. 122761)
abridges@fenwick.com
MEGHAN E. FENZEL (CSB No. 324139)
mfenzel@fenwick.com
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Telephone: 650.988.8500
Facsimile: 650.938.5200

JEDEDIAH WAKEFIELD (CSB No. 178058)
jwakefield@fenwick.com
SAPNA MEHTA (CSB No. 288238)
smehta@fenwick.com
MATTHEW B. BECKER (CSB No. 291865)
mbecker@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile: 415.281.1350

Attorneys for Defendant
CLOUDFLARE, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

(SAN FRANCISCO DIVISION)

MON CHERI BRIDALS, LLC, *et al.,*

Plaintiffs,

v.

CLOUDFLARE, INC., and DOES 1–500, Inclusive,

Defendants.

Case No.: 19-cv-01356-VC

DEFENDANT CLOUDFLARE, INC.'S NOTICE OF CROSS-MOTION AND BRIEF IN SUPPORT OF ITS CROSS-MOTION FOR SUMMARY JUDGMENT AND OPPOSITION TO PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

Date: September 16, 2021
Time: 10:00 a.m.
Courtroom: 4
Judge: Hon. Vince Chhabria

Redacted Version of Document Sought to Be Sealed

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(Continued)

Page(s)

STATUTES AND RULES

TABLE OF AUTHORITIES
(Continued)

Page(s)

OTHER AUTHORITIES

NOTICE OF CROSS-MOTION AND MOTION

Defendant Cloudflare, Inc. hereby moves for summary judgment against Plaintiffs and will present the motion on September 16, 2021, at 10:00 a.m., on the following grounds: (1) Plaintiffs cannot establish contributory infringement by Cloudflare; (2) Plaintiffs cannot establish ownership and valid, timely registration of any of the copyrights they assert; (3) Plaintiffs cannot establish they are entitled to any relief because (a) the safe harbors under 17 U.S.C. §§ 512(a) and 512(b) for online service providers preclude any monetary relief, (b) Plaintiffs cannot establish entitlement to the statutory damages they have elected, and (c) Plaintiffs cannot show irreparable harm from Cloudflare to justify an injunction; and (4) Plaintiffs cannot establish direct infringement liability of the 500 Doe defendants they never named or served.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs brought this lawsuit based on a fundamental misunderstanding of Cloudflare's services, the contributory copyright infringement doctrine, and the Digital Millennium Copyright Act, all in pursuit of a statutory damages windfall that has nothing to do with the harm they claim to have suffered. Plaintiffs are two wedding and formal dress vendors whose complaint at its core is that unnamed Doe defendants allegedly sold knockoff versions of their dresses online. Rather than attack the sale of those dresses, Plaintiffs seek to collect damages based on images allegedly used to market them. And rather than pursue relief against the Doe defendants on whose websites they claim the images appeared (or the hosting providers, ISPs, and domain registrars actually essential to their websites' operations), Plaintiffs target Cloudflare, a cybersecurity company that protects from malicious attacks tens of millions of websites, including those of the Doe defendants (as well as Plaintiff Maggie Sottero Designs). In doing so, Plaintiffs seek an expansion of the contributory infringement doctrine far beyond its established limits and try to pin liability where it does not belong.

Contributory copyright infringement cannot arise from the limited and generally available services Cloudflare provided in this case, and Plaintiffs cannot show the culpable conduct required

to impose liability. Cloudflare is nothing like the search engines and peer-to-peer networks that the Ninth Circuit has found "significantly magnify otherwise immaterial infringements." Whereas Cloudflare's services protect against malicious attacks and at most confer a split-second advantage to the loading time of a website someone is already visiting, the services previously considered by the Ninth Circuit actually helped visitors find infringing material they otherwise never would have found. There also is no "simple measure" that Cloudflare failed to take to prevent further infringements in this case. Unlike hosting providers, Cloudflare could not remove allegedly infringing material from the Internet, and there is no question that those images would have remained available and equally accessible on the accused websites without Cloudflare's services. Finally, even if termination of Cloudflare's services could ever be justified, it would not have been proper based on the faulty notifications of claimed infringement submitted by Plaintiffs' agent, which has a contingency interest in this case and a track record of unreliability already recognized by a federal court. Plaintiffs therefore cannot show Cloudflare had the actual knowledge of infringements required for contributory infringement liability.

Similar errors underlie other fatal flaws in Plaintiffs' case. They ignore the two safe harbors from liability in the Digital Millennium Copyright Act 17 U.S.C. §§ 512(a), (b), that specifically apply to Cloudflare's conduit and caching services and that would bar any relief against Cloudflare even if it could be deemed a contributory infringer. They also ignore the most basic elements for suing and claiming statutory damages. Plaintiffs cannot show copyright ownership. Nor can they prove they registered the copyrights before alleged infringements began, which is a prerequisite for statutory damages.

The Court should grant summary judgment to Cloudflare and deny the Plaintiffs' motion.

II. BACKGROUND

A. The Internet and Cloudflare's Place in It

Cloudflare was founded to protect against the rising threat of malicious cyberattacks. Cloudflare's services at issue in this case operate (along with many other third-party services) between its customers' websites and users who want to reach those websites. Internet traffic to and

from those websites passes through Cloudflare's system, as one link in a chain of transmissions, so that Cloudflare's system can detect and interrupt threats. Guinn Decl. ¶¶ 10, 14. Cloudflare both protects its customers (and their users) from attacks and prevents them from becoming vectors for further attacks. *Id.*; Schneier Decl. ¶¶ 3–22; Schonfeld Decl. ¶¶ 19–22. While Cloudflare makes money primarily from large enterprise customers, it offers free services to millions of customers, protecting both the customers and the Internet as a whole. Guinn Decl. ¶¶ 3, 29. Cloudflare's network transmits approximately ten percent of all Internet traffic, and it constitutes a major component of the Internet's infrastructure. *Id.* ¶ 3.

To use these services, a customer must already have a website, a web hosting provider, a domain name registrar, and an ISP to connect the hosting service and the Internet. Guinn Decl. ¶¶ 10, 20. In other words, the customer's website must already be up and running online. Only then can customers direct traffic to their websites through Cloudflare's network, by substituting a Cloudflare Internet Protocol (IP) address for their web host's IP address. *Id.* ¶¶ 12–13. This "reverse proxying" service acts like a detour for Internet traffic that would otherwise pass directly to the customer's website, providing an important safeguard against attacks. *Id.* ¶¶ 13–14; Schonfeld Decl. ¶ 12; Schneier Decl. ¶¶ 15–22. Cloudflare cannot inspect the *content* of materials that cross its network, but its technology can identify and block malicious traffic *patterns* before they reach website hosts. Guinn Decl. ¶¶ 14, 30–33.

Because adding threat detection to Internet traffic can slow it, security services historically sought to compensate for it by improving Internet performance. Guinn Decl. ¶ 21. Cloudflare does so by operating a content delivery network (CDN) and providing other services to help the Internet work faster and more efficiently. *Id.* ¶ 22. Like other CDN providers, Cloudflare uses many "points of presence" globally that "cache," or temporarily mirror, materials that users frequently request from customer websites. *Id.* ¶¶ 13, 22; Schonfeld Decl. ¶¶ 13–15. This both protects against attacks and makes the Internet more efficient by reducing the distance that the data must travel. *Id.* ¶¶ 18, 28. Because customer websites are always changing, Cloudflare's caching function frequently "refreshes" material to match changes at the originating websites. Guinn Decl. ¶ 24. Because the

cache merely reflects what is hosted on the website, removing material from a website host will remove it from Cloudflare's cache, but removing it from Cloudflare's cache does not remove it from the source website. *Id.* ¶ 39.

Cloudflare also helps website performance by streamlining transmissions without altering the substance, or "content," of any material. This includes compression (making files smaller), smart routing (using the most efficient routes), and other similar features. *See* Guinn Decl. ¶¶ 15, 45. Like other CDNs, Cloudflare's services improve Internet traffic by requiring less bandwidth, avoiding bottlenecks, and reducing congestion. *Id.* ¶ 22; Schonfeld Decl. ¶ 68. Cloudflare's caching and optimization functions can also improve web page loading speed, typically by fractions of a second. Guinn Decl. ¶¶ 27, 28. Countless other factors have greater impacts on webpage speed than Cloudflare's offerings, including the type of Internet service provider, personal devices used, distance from a cell tower or WiFi router, and the number of people sharing a router or network. *Id.* ¶ 27; Schonfeld Decl. ¶ 65.

None of the services Cloudflare provided to the websites at issue in this case enable infringements. Cloudflare neither provided access to the Internet nor hosted those websites. Other companies provide those services, such as Comcast/Xfinity for Internet access and Bluehost for website hosting. Guinn Decl. ¶ 35. Nor did Cloudflare provide any domain registration service, like that of Register.com, so that the public can find the websites at issue by name. *Id.* ¶ 36.c. Nor does Cloudflare provide a search engine, like Google, to allow Internet users to find online material, or a storage platform for access to material, such as YouTube, Facebook, or Dropbox. *Id.* ¶¶ 36.a, 36.d. Nor does Cloudflare provide payment processing, shipping, or other services that allow accused counterfeiters to run their businesses. *Id.* ¶ 36.e.

Cloudflare does not specialize in any type of customer or material: it provides general-purpose services to over 25 million web properties, including governments, political candidates, utilities, dissident groups challenging authoritarian governments, retailers, law firms, labor unions, universities, and countless other types of businesses and organizations. Guinn Decl.¶ 3.

B. Cloudflare's Policies and Practices for Handling Abuse Complaints

Cloudflare's reverse proxy security function causes Cloudflare IP addresses to appear in public records for websites of Cloudflare customers. Paine Decl. ¶ 6. As a result, some parties send Cloudflare complaints for its customers' hosting providers, including copyright complaints. *Id.* Cloudflare provides a web form for submission of copyright complaints, which it uses to collect and forward information to the web hosting providers and website operators who, unlike Cloudflare, can remove or disable access to materials or address accusations of infringement. *Id.* ¶¶ 5–7, 11. Cloudflare advises complainants that, "Because Cloudflare does not have the ability to remove content from a website, it is our practice to forward abuse complaints to entities like the hosting provider and/or website owner to follow up." *Id.* ¶ 7, Ex. 2. The web form triggers an automated process that does two things. First, it transmits the complaint to the website owner, the website hosting provider, or both at the complainant's option. *Id.* ¶ 8. Second, it responds to the complainant, giving the name and contact information for the relevant hosting provider so that the complainant can take further action. *Id.* ¶ 10. In addition, as Cloudflare describes below, Cloudflare reasonably implemented a policy for terminating services to repeat infringers in appropriate circumstances. Paine Decl. ¶¶ 20–24.

C. The Plaintiffs, Their Litigation History, Their Contingent-Fee Witnesses, Their Communications with Cloudflare, and Cloudflare's Responses

Plaintiffs import and sell wedding or other special-occasion dresses through retail dress shops in the United States. They are members of the American Bridal and Prom Industry Association (ABPIA), which [redacted] Dkt. 2. Lead Plaintiff Mon Cheri Bridals [redacted] Bridges Decl. ¶¶ 5.a–c, Ex. 4; ¶ 16, Ex. 15; ¶¶ 28–45, Ex. 24–41.

ABPIA and its members, including Plaintiffs, have brought dozens of lawsuits in federal courts against thousands of "Doe" defendants, allegedly website owners or operators that use the plaintiffs' brands or images to sell knockoff dresses. Counsel for Plaintiffs in this case have publicized ABPIA's success, claiming to have shut down over 2,000 websites through litigation.

Bridges Decl. ¶ 16, Ex. 15. The lawsuits follow a common pattern: (1) complaints identify websites alleged to have infringed trademarks or copyrights, (2) the plaintiffs obtain TROs against the websites, (3) the plaintiffs obtain expedited discovery through subpoenas to websites' various service providers, (4) the plaintiffs freeze financial accounts of the websites, (5) the plaintiffs obtain addresses of the websites and serve them with process, (6) the plaintiffs obtain preliminary injunctions blocking the websites and transferring control of their finances and domain names, and (7) the plaintiffs obtain default judgments and permanent injunctions putting the websites out of business. *See* Bridges Decl. ¶¶ 5.a–c, Ex. 4; *see also* ¶¶ 28–45, Ex. 24–41.

In earlier lawsuits, ABPIA and Plaintiffs identified a wide range of online services that were critical to the operation of those infringing websites or held key information about them. They included domain registrars, domain registries, web hosting providers, web designers, third-party selling platforms, search engines, ad-word providers, payment processors and financial institutions, and shippers. Plaintiffs' papers in other suits specifically mentioned PayPal, Western Union, MasterCard, Visa, VeriSign, Neustar, and Public Interest Registry; in addition, they sought TROs, preliminary injunctions, and permanent injunctions against not only the defendants in those cases but also against all persons with notice of the orders and in active concert or participation with those defendants. Bridges Decl. ¶¶ 28–45, Ex. 24–41. They never mentioned Cloudflare.

Before this lawsuit, Plaintiffs never identified Cloudflare in any litigation as facilitating allegedly infringing websites, never sought relief against Cloudflare, never served injunctions on Cloudflare, and never notified Cloudflare of those lawsuits. Paine Decl. ¶ 27; Bridges Decl. ¶ 3.a, Ex. 2. They also never subpoenaed Cloudflare for information about customers, even though Cloudflare regularly responds to valid subpoenas for customer information. Paine Decl. ¶¶ 15, 27; Bridges Decl. ¶ 5.d, Ex. 4; *see also* 17 U.S.C. § 512(h) (DMCA subpoena provision). To Cloudflare's knowledge, Plaintiffs also never sued any of the third-party service providers they had identified in earlier lawsuits as facilitating the accused websites. Now they sue Cloudflare, relying primarily on the efforts of witnesses who themselves have a contingency interest in windfall statutory damages or settlement of this lawsuit. Bridges Decl. ¶¶ 2.a, Ex. 1; 4.a, Ex. 3.

Plaintiffs' contingency-fee witnesses are Suren Ter-Saakov and Armen Petrossian, principals of XMLShop LLC, which goes by the name "Counterfeit.Technology." Neither is qualified or was even disclosed as an expert. Bridges Decl. ¶¶ 2.f. and 3.c. Mr. Ter-Saakov claims to have directed freelancers to develop technology for uncovering alleged infringements and sending accusations to online services. He claims Mr. Petrossian used the technology to generate accusations that go out under Mr. Petrossian's name, but "the technology," not Mr. Petrossian, is the author of the accusations. XMLShop is not compensated for sending accusations to Cloudflare. Instead it will receive a payout, if at all, only from this lawsuit. Bridges Decl. ¶ 2.a, Ex. 1. Thus, XMLShop's incentive was to set up this lawsuit, not to take effective measures against alleged infringers. *See id.*

Cloudflare responded to XMLShop's notifications of claimed infringement in several ways, following its standard processes. First, when XMLShop sent accusations by email, Cloudflare automatically responded by directing XMLShop to Cloudflare's online web form. When XMLShop used that online webform, Cloudflare automatically (1) forwarded the complaint to the customer's hosting provider for the website with accused material; (2) notified the customer; and (3) responded to XMLShop.

III. ARGUMENT

A. Cloudflare Has Not Engaged in Contributory Infringement.

Plaintiffs cannot show that Cloudflare enabled or materially assisted the alleged copyright infringements, let alone with the culpable intent that is a prerequisite of contributory infringement liability. Cloudflare's security and performance services are both capable of, and are widely used for, non-infringing purposes. *See* Dkt. 124-1 at 1; Guinn Decl. ¶ 3. Several points are beyond genuine dispute. Accused websites would have remained available without Cloudflare's services; Cloudflare's services were just one (non-essential) link in a long chain of transmission; the services at most would marginally increase those websites' loading speed; and Cloudflare cannot remove any customer content from the Internet. Guinn Decl. ¶ 37. Moreover, Cloudflare has a system for forwarding copyright complaints to those who actually can remove content: the website operators

and their hosting providers. Paine Decl. ¶¶ 7–9; Bridges Decl. ¶ 23.b, Ex. 19. Cloudflare's system worked to forward the complaints XMLShop submitted, and XMLShop never submitted additional facts (such as an adjudication of infringement or evidence that material had been removed at the host) specifically tailored to the caching services Cloudflare provided. Paine Decl. ¶¶ 25–26. Given those facts, Plaintiffs cannot satisfy their burden of showing that Cloudflare materially assisted infringements with "purposeful, culpable expression and conduct," *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 937 (2005). The Court should grant summary judgment to Cloudflare.

1. Contributory Infringement Requires Culpable Intent.

Consistent with the common law rules of fault-based liability from which it emerged, contributory copyright infringement requires a showing of "purposeful, culpable expression and conduct" such that "mere knowledge of infringing potential or of actual infringing uses would not be enough." *Grokster, Ltd.*, 545 U.S. at 937; *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 794–95 (9th Cir. 2007). Under those common law principles, so long as a technology is "capable of substantial noninfringing uses," the mere fact that the technology might also be used by an infringer does not mean that the sale of the technology "constitute[s] contributory infringement." *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984). The "well-settled rule" the Supreme Court outlined in *Grokster* is that "one infringes contributorily by *intentionally* inducing or encouraging direct infringement." *Cobbler Nevada, LLC v. Gonzales*, 901 F.3d 1142, 1147 (9th Cir. 2018) (emphasis added) (quoting *Grokster*, 545 U.S. at 930, and *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1170 (9th Cir. 2007)). The requisite intent must be clear: contributory infringement requires "clear expression or other affirmative steps taken to foster infringement." *Cobbler Nevada* , 901 F.3d at 1148 (quoting *Grokster*, 545 U.S. at 919).

"Consistent with the rule set forth in *Grokster*," *Amazon.com*, 508 F.3d at 1171, the Ninth Circuit has offered "non-contradictory variations on the same basic test." *Visa,* 494 F.3d at 795. The Court stated in *Visa* that "one contributorily infringes when he (1) has knowledge of another's infringement and (2) either (a) materially contributes to or (b) induces that infringement." *Visa*,

494 F.3d at 795; see also *id*. (rejecting claim against Visa and cautioning that "the language of the tests" should not be read "broad[ly]," such that they "would require a radical and inappropriate expansion of existing principles of secondary liability"). The court has found liability when the defendant "engages in *personal* conduct that encourages or assists the infringement." *Id.* (quoting *Napster*, 239 F.3d at 1019). The court also explained that "a computer system operator is liable under a material contribution theory of infringement if it has actual knowledge that specific infringing material is available using its system, and can take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works." *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 671 (9th Cir. 2017) (cleaned up) (quoting *Amazon.com*, 508 F.3d at 1172). Regardless of the wording to describe the test, the Ninth Circuit has repeatedly recognized that the touchstone of contributory infringement must be *active, culpable intent*.

2. Plaintiffs Cannot Satisfy Their Burden of Demonstrating that Cloudflare Materially Assisted Infringement with Culpable Intent.

Against this backdrop, Plaintiffs cannot establish contributory infringement by Cloudflare. The crux of Plaintiffs' argument is that Cloudflare provides caching and optimization services that might improve websites' load times. Plaintiffs concede that "many legitimate websites use Cloudflare's services (including one of the Plaintiffs)," [1] Dkt. 124-1 at 1, and knowledge that its general-purpose services will sometimes be used for infringement cannot establish Cloudflare's culpable intent necessary for contributory infringement. *Grokster*, 545 U.S. at 935.

Plaintiffs cannot establish any of the three elements the Ninth Circuit has required for imputing culpable intent. *First*, Plaintiffs cannot show Cloudflare's services materially contribute to alleged infringements, as they do not "significantly magnify" otherwise immaterial

[1] Notably, Plaintiffs did not move for summary judgment on the basis that Cloudflare materially contributes to infringements by "hiding" infringers' identities. *See* Dkt. 124-1 at 22–23. This differs from their initial allegations, which the Court had found sufficient to state a claim. Dkt. 54 at 1. Following discovery, it is undisputed that Cloudflare provides the identities of alleged infringers in response both to abuse reports and valid legal process. *Cf. id.; see also Rosen v. Imagevenue.com*, No. CV-13-01742-SJO(MANx), 2013 WL 12132052, at *5 (C.D. Cal. Nov. 26, 2013) (dismissing contributory infringement claim against WHOIS database privacy service for offering privacy services).

infringements. *Second*, Cloudflare responds properly to allegations of infringement, and Plaintiffs cannot show that Cloudflare failed to take any other "simple measures" to prevent further infringements. *Third,* Plaintiffs cannot show that Cloudflare had actual knowledge of infringements sufficient to justify the actions they suggest Cloudflare should have taken.

a. Cloudflare Does Not Materially Contribute to Infringements.

Plaintiffs cannot show that Cloudflare materially contributes to infringements. The Ninth Circuit has refused to extend "material contribution" to include "any tangible or intangible component related to any transaction in which infringing material is bought and sold." *Visa*, 494 F.3d at 799–800. Instead, the court limited material contributions to those services or actions that "significantly magnify the effects of otherwise immaterial infringing activities." *Amazon.com*, 508 F.3d at 1172; *cf. Flava Works Inc. v. Gunter*, 689 F3d 754, 757 (6th Cir. 2012) (Posner, J.) (asking whether one can "materially contribute to something without causing or inducing it").

Cloudflare's services do not "significantly magnify the effects" of immaterial infringements on customer websites. While Plaintiffs focus on load times, they have no evidence of a speed difference for any image at issue in this case. Bridges Decl. ¶ 8.a, Ex. 7; Schonfeld Decl. ¶¶ 63–66. Regardless, a split-second difference in an image's load time is vastly different, quantitatively and qualitatively, from the benefit of services the Ninth Circuit has identified as potential material contributions. Google search made "immaterial infringements" material by "significantly magnifying" them, allowing users (in seconds) to find materials they otherwise would likely never find, or that would take hours or days to locate. *See Visa*, 494 F.3d at 798–99 (discussing *Amazon.com* and highlighting how search engines work "with astounding speed"). Likewise, the P2P services in *Napster* and *Grokster* "allowed users to locate and obtain infringing material" that would otherwise be unavailable. *Id*. at 796.

In contrast, Cloudflare makes no "otherwise immaterial infringements" become material. Unlike with search engines and P2P services, user actions are the same with or without Cloudflare; all that changes is the traffic path through the Internet and possibly a split-second difference in image loading. Guinn Decl. ¶¶ 27–28. The alleged displays would occur regardless of Cloudflare.

Id. ¶ 32. Plaintiffs' own expert drives this point home. He admitted he easily accessed an image on an accused website that was *not* in Cloudflare's cache. Bridges Decl. ¶ 8.a, Ex. 7. That should end the inquiry: a service does not *materially* contribute to infringement when, without the service, "there would still be infringement." *See Visa*, 494 F.3d at 796; *Flava Works*, 689 F.3d at 759.

Plaintiffs speculate that improvements in website speed, generally, may contribute to a better user experience, which, in turn, may contribute to improved "conversion" (the rate at which customers complete purchases). But Plaintiffs claim infringements in displays of images, not in sales of dresses (in which Plaintiffs cannot claim any copyrights). Regardless, they offer no competent evidence of any such effect on any of the websites in this case. Moreover, *Visa* recognized that payment processors, who are vital to every online commercial transaction and make instant transactions possible, are not contributory infringers. *Visa,* 494 F.3d at 795, 801. Even more tenuously related services like Cloudflare's cannot support a finding of a "purposeful, culpable" contribution to infringement. Plaintiffs disregard the Ninth Circuit's caution in *Visa* against the "radical and inappropriate expansion" of secondary liability to attack services that do not cause or make a material difference to infringement. *See id.* at 795. Their contributory infringement claim fails.

b. Cloudflare Took Appropriate Measures.

For related reasons, Plaintiffs' claim also fails because they cannot identify any "simple measures" that Cloudflare should have taken, but did not take, to prevent alleged infringements. The Supreme Court has cautioned that "mere[] . . . failure to take affirmative steps to prevent infringement" is generally insufficient to establish secondary liability. *Grokster, Ltd.*, 545 U.S. at 939 n.12. The Ninth Circuit has reasoned that the failure to "take simple measures to prevent further damage to copyrighted works" despite "actual knowledge" of "specific infringing material" may be a basis for secondary liability in some circumstances. *Giganews*, 847 F.3d at 671 (quoting *Amazon.com*, 508 F.3d at 1172). Given *Grokster*'s clear rule requiring culpable conduct, however, any such "simple measure" must be one that is so "reasonable and feasible" that culpable intent can be inferred from the mere fact of not deploying it. *Amazon.com*, 508 F.3d at 1172–73.

Cloudflare cannot stop infringements for the reasons already discussed: it is merely one link in the chain of transmissions, and not a necessary one at that. *See* Guinn Decl. ¶ 37. By forwarding Plaintiffs' complaints to website operators and their hosting providers, and by providing host information to XMLShop, Cloudflare took the only simple measures available. Paine Decl. ¶¶ 6–7, 25; Bridges Decl. ¶ 23.b, Ex. 19; Schonfeld Decl. ¶¶ 59–60. The Ninth Circuit recently ruled that a service provider's forwarding of complaints to customers satisfied the "simple measures" test. *See ALS Scan, Inc. v. Steadfast Networks, LLC*, 819 F. App'x 522, 523 (9th Cir. 2020). Cloudflare's responses were precisely the measures appropriate for an internet infrastructure provider that does not "operate, control, or manage any functions of" its customers. *Id*.

Plaintiffs cannot identify other "reasonable and feasible steps" Cloudflare could have taken but failed to take. In particular, while Plaintiffs seem to think Cloudflare should terminate all services any time it receives some unspecified number of allegations of infringement, that would not actually prevent infringements and could have severe consequences. *See* Dkt. 124-1 at 21. Websites with terminated services would remain available online but be left unsecured from cyberattack, making the broader internet less safe. Bridges Decl. ¶ 8.b, Ex. 7; Paine Decl. ¶ 22; Schneier Decl. ¶¶ 31–39; Schonfeld Decl. ¶¶ 58, 61. And any protocol of terminations resulting from mere accusations would invite malicious actors to abuse the process. Paine Decl. ¶¶ 17–19; Schneier Decl. ¶¶ 23–28. Just as a burglar first cuts a security camera and home alarm, malefactors would use a flurry of copyright complaints to eliminate cybersecurity protections for their targets.

Plaintiffs suggest alternatively that Cloudflare could have (1) purged its cache servers of the accused content; (2) disabled caching services to an accused domain or URL; (3) blocked public access to the accused content; and/or (4) ceased providing website optimization services to an accused domain. Dkt 124-1 at 20–21. But Plaintiffs do not explain how these are "reasonable and feasible" or, more importantly, how they would "prevent further damage to copyrighted works." *See Amazon.com*, 508 F.3d at 1172. None of Plaintiffs' proposals withstands scrutiny.

Plaintiffs' first suggestion, purging accused content from caches, does not hinder access to content that still resides at the originating website. Paine Decl. ¶ 12; Guinn Decl. ¶¶ 24, 39; Schonfeld Decl. ¶ 62. That is why Section 512(b) of the DMCA—the framework and safe harbor from liability Congress provided to address these issues—requires notifications to caching providers to state that the material has been removed from the originating site or that a court has ordered that to happen. 17 U.S.C. § 512(b)(2)(E). Cloudflare *does* purge caches in response to such statements, but Plaintiffs never provided those required statements in any notifications, and apparently did not follow up with the hosting providers to seek removal of material at the source. Paine Decl. ¶¶ 12, 26; Bridges Decl. ¶ 22.

For similar reasons, Plaintiffs' second and fourth suggestions, disabling caching or any other "optimization services," also would not prevent alleged infringements so long as the images remain available at the host.[2] Guinn Decl. ¶ 43. Moreover, even if Cloudflare had the technical ability to disable caching on a URL by URL basis, that action would easily be evaded by its customers, and disabling caching for an entire website has some of the same security implications as terminating other services. Guinn Decl. ¶¶ 42–43; Paine Decl. ¶ 21; Schneier Decl. ¶ 42; Schonfeld Decl. ¶ 62. Consequently, while Cloudflare will sometimes disable caching and related services, it is not a "simple measure," and the mere failure to do so cannot establish any culpable intent on the part of Cloudflare to foster infringement. Measures that are "onerous and unreasonably complicated" or "unreliable and burdensome" are not simple measures. *Giganews*, 847 F.3d at 671. And a measure that fails to "prevent further damage to the copyrighted works" cannot be necessary. *See id.*

Finally, Plaintiffs' suggestion that Cloudflare should affirmatively block content altogether is simply a nonstarter. It is not technically feasible for Cloudflare to block specific material on websites in response to all copyright complaints. Bridges Decl. ¶ 9.a, Ex. 8; Guinn Decl. ¶ 42; Schonfeld Decl. ¶ 56. And while Plaintiffs suggest that Cloudflare could hack into and manipulate

[2] Plaintiffs' suggestion that Cloudflare terminate other optimization services is a red herring. Cloudflare offers very little optimization other than caching to free and self-serve customers. Almost all of the accused infringing domains used Cloudflare's free services. Paine Decl. ¶ 28.

its customers' security settings to put up a firewall to block all access to the site, this step is not only drastically disproportionate but it also would be ineffective. *See* Guinn Decl. ¶ 42; Schneier Decl. ¶ 40. Any customer facing such an attack from its own security service would quickly stop using that service and get back online. *Id.* This is because, unlike other Internet services that a Cloudflare customer must have, Cloudflare's services are not essential to any acts of infringement. *See* Guinn Decl. ¶ 37; Schonfeld Decl. ¶¶ 52–54.

In all events, blocking access to an entire website because of certain accused photos is a blunt and overbroad remedy not proportional to the harm. *Perfect 10, Inc. v. Google, Inc.*, No. CV 04-9484 AHM (SHx), 2010 WL 9479060 (C.D. Cal. July 30, 2010), aff'd, 653 F.3d 976 (9th Cir. 2011). Terminating *all* services or blocking all traffic (even if possible) to an accused customer's web server is even more extreme. *See* Dkt. 124-1 at 15–16 (citing Jonyer Rep. Ex. EE at 62). Stripping websites of security jeopardizes the Internet, Paine Decl. ¶¶ 19, 22, and extreme responses are not "reasonable and feasible," particularly in response to unadjudicated accusations of infringement. That Cloudflare does not take *unreasonable*, *infeasible,* and ultimately *ineffective* measures cannot establish intent—"purposeful, culpable" complicity in copyright infringements.

Even valid copyright interests cannot justify, as a "simple measure," that a legitimate company undermine its very service to "make it easier for copyright holders to obtain satisfaction." *Rosen*, 2013 WL 12132052 at *5. Cloudflare already acts appropriately upon notifications of claimed infringement. Paine Decl. ¶¶ 7–10; Bridges Decl. ¶ 23.b, Ex. 19. Plaintiffs cannot identify any other steps so reasonable and obvious that Cloudflare's failure to take them shows it to be a culpable, purposeful contributory infringer.

c. XMLShop's Communications Did Not Give Actual Knowledge of Specific Infringements.

Even if any of Plaintiffs' proposals could ever be appropriate "simple measures" in response to claims of infringement, Plaintiffs cannot show Cloudflare had "actual knowledge of specific infringing activities" to trigger such measures. *Amazon.com*, 508 F.3d at 1176. This is particularly true given the history of unreliable infringement accusations, the risk of their abuse to

undermine legitimate security services, and the particular flaws in the notices of Plaintiffs' own copyright agent XMLShop. *See* Paine Decl. ¶¶ 18, 19; Bridges Decl. ¶ 15, Ex. 14; ¶ 43, Ex. 39.

Notifications of claimed infringement provide actual knowledge of only one thing—that someone has made a *claim* of infringement. That might be sufficient grounds for a hosting provider to remove content from its servers within the DMCA framework, but even then, the DMCA provides that the host should give its customer an opportunity to dispute the infringement allegation and restore the content. 17 U.S.C. §§ 512(f), 512(g)(2)(C). Cloudflare does not host the accused websites, it could not remove content in response to Plaintiffs' complaints, and it cannot adjudicate disputes between claimants and customers. Paine Decl. ¶¶ 4, 5, 17. Moreover, copyright owners bear the burden to investigate alleged infringers, and the law "impose[s] no such investigative duties on service providers." *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007). In that context, and without any order adjudicating a customer as an infringer, Cloudflare had no knowledge to justify the blunt, domain-level actions—based only on unvalidated allegations—that Plaintiffs suggest Cloudflare should have taken.

That is especially true given the unreliability of infringement accusations. Schneier Decl. ¶¶ 26–27. Recent scholarship reflects how "nearly every OSP" sees abuse frequently in the DMCA notice and takedown system. *See* Jennifer M. Urban, Joe Karaganis & Brianna L. Schofield, *Notice and Takedown in Everyday Practice* 40 (2016). Some malicious actors even forge court documents to prod service providers into acting against their customers, and Cloudflare has received such fake notifications. *See* Eugene Volokh, *Shenanigans (Internet Takedown Edition)*, available at https://www2.law.ucla.edu/volokh/shenanigans.pdf (forthcoming in Utah Law Review).[3] As a security service provider, Cloudflare is wary of incomplete notifications and must be cautious even when receiving seemingly valid notifications. If malicious actors can use false notifications to remove Cloudflare's protective shield, that enables their attacks. Paine Decl. ¶¶ 17–19.

[3] Section 512(f) also recognizes that seemingly valid notifications may contain misrepresentations. 17 U.S.C § 512(f) (providing for damages and attorneys' fees for persons injured by removing or disabling access to material falsely claimed to be infringing); *see also Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2015) (permitting claim to proceed against copyright owner for failing to consider fair use in sending DCMA notifications).

Indeed, these very problems exist in this case, and the notifications of Plaintiffs' own copyright agent XMLShop's have multiple signs of unreliability. XMLShop's communications to Cloudflare on behalf of Plaintiffs had confusing inaccuracies that caused Cloudflare to question the reliability of all correspondence from XMLShop. *See* Bridges Decl. ¶ 14, Ex. 13. Domain registrants similarly struggled with bombardment of boilerplate and improper notifications from XMLShop. *See* Bridges Decl. ¶ 15.a, Ex. 14 ("we have received numerous emails that were either 'spam' or not actionable"). Mr. Ter-Saakov himself reluctantly acknowledged that "false positive [are] always a problem." *See* Bridges Decl. ¶ 2.e, Ex. 1. And when Federal District Court Judge Blakey expressed concern in another case about the diligence behind accusations by XMLShop, Mon Cheri, and ABPIA and demanded explanations of the "numerous false-positives in the results," they tried to dismiss the Doe defendants to avoid having their complaint system exposed. Bridges Decl. ¶ 43, Ex. 39. Judge Blakey later issued a long opinion criticizing the software's accuracy and opining that "Counterfeit Technology's anti-counterfeiting software program . . . . does not, without more, constitute proof of actual counterfeiting." *Id.* at 9. Judge Blakey did not credit the declaration of Mr. Ter-Saakov, who is also a declarant for Plaintiffs here. *Id.* at 7. Thus, XMLShop's notifications provide only dubious *accusations* and cannot convey actual knowledge of specific acts of infringement. *See Amazon.com*, 508 F.3d at 1172.

XMLShop's notifications suffered from the additional flaw that they were directed towards hosting providers, not a caching and conduit provider such as Cloudflare.[4] *See* Paine Decl. ¶¶ 25–26, Ex. 10. While a provider like Cloudflare might be expected to purge its cache in response to proper notifications, that would only be the case when the provider knows that the allegedly infringing content has been removed at the host such that purging cache would be effective. *See* Paine Decl. ¶ 12. That is precisely why notifications to caching providers under Section 512(b) must confirm that the material has been removed from or disabled on the originating site, or that a

[4] As discussed above, although doing so is not a condition to qualify for the safe harbor, Cloudflare forwarded the information in the notifications to hosting providers and customers, and identified the hosting provider to Plaintiffs, enabling Plaintiffs and the hosting providers for the accused websites to interact directly, as 17 U.S.C. § 512(c) envisions.

court has ordered that to happen. 17 U.S.C. § 512(b)(2)(E). But Plaintiffs *never* provided a notification to Cloudflare with such a statement, and they have never forwarded a court order regarding a customer's infringement. Bridges Decl. ¶ 3.a, Ex. 2. At most, Plaintiffs' notifications supplied the necessary information for a hosting provider. Well into the case, after Cloudflare had explained the deficiencies of the notices, Plaintiffs' counsel instructed XMLShop to modify its notifications. Later notifications specifically addressed Cloudflare and omitted reference to section 512(c). But they failed to mention section 512(b) and made no effort to comply with Section 512(b)(2)(E)(ii) despite knowledge of its requirements. Bridges Decl. ¶ 2.g., Ex. 1; *see generally* Dkt. Nos. 124-60 to 124-62 (notifications of claimed infringement).

Plaintiffs' notifications are therefore invalid and cannot serve as evidence of actual knowledge. Indeed, the Ninth Circuit has held that improper notifications under the DMCA do not provide actual knowledge of specific acts of infringement. *See Luvdarts, LLC v. AT & T Mobility, LLC*, 710 F.3d 1068, 1072–73 (9th Cir. 2013) (dismissing for faulty notifications). And the Ninth Circuit model jury instruction for the Section 512(b) safe harbor for caching providers states: "If the notification does not meet all the above requirements, then it is invalid and cannot be used as evidence of the defendant's knowledge of specific infringing activity." Ninth Circuit Model Jury Instructions 17.29 Copyright—Affirmative Defense—Limitation on Liability for System Caching (17 U.S.C. § 512(b)). Plaintiffs' claims fail on that basis alone.

B. Plaintiffs Fail to Prove Copyright Ownership.

Copyright registrations provide only *prima facie* evidence of validity and of facts (like ownership) in the certificate. 17 U.S.C. § 410(c). Here, abundant evidence contradicts Plaintiffs' claim of ownership, and none of the Plaintiffs' documents are evidence of ownership.

A creator of a work—here, a photographer, not Plaintiffs—originally owns copyright in a work unless it is a "work made for hire." 17 U.S.C. § 201. That status arises from actual employment of the creator or, for certain types of works, from a written agreement signed by both parties and meeting a number of conditions. 17 U.S.C. § 101 ("work made for hire" definition). Plaintiffs registered their images as works made for hire. Dkts. 124-58; 124-59. They did not

employ the photographers. Bridges Decl. ¶ 7.b, Ex. 6. Nor do they have any valid agreements: [redacted][5] Bridges Decl. ¶ 5.f, Ex. 4; ¶ 7.e, Ex. 6; ¶ 18, Ex. 17; ¶ 19, Ex. 18.

Nor do the agreements evidence transfer of ownership. §§ 201(d), 204(a). Almost all of Mon Cheri's disclosed agreements either do not define "the Company" to which rights shall be assigned or define the *photographer* as the assignee. Bridges Decl. ¶ 18, Ex. 17. And they purport to cover only four of the titles in Plaintiffs' registration certificates. *Compare* Dkt. 124-58, *with* Bridges Decl. ¶ 18, Ex. 17. None of Maggie Sottero's agreements [redacted] Bridges Decl. ¶ 19, Ex. 18; *see also* Dkt. 124-59. They recite a [redacted]. *Id.* [redacted] *Id.*

"The rule is really quite simple: If the copyright holder agrees to transfer ownership to another party, that party must get the copyright holder to sign a piece of paper saying so." *Gladwell Gov't Servs., Inc. v. Cty. of Marin*, 265 F. App'x 624, 626 (9th Cir. 2008) (citation and internal quotation marks omitted). Plaintiffs did not do so. Their "agreements" purporting to show their ownership are insufficient on their face, and the Court should deny Plaintiffs' motion for summary judgment and enter summary judgment for Cloudflare on ownership.

C. Plaintiffs Are Not Entitled to Any Relief.

Apart from the substantive question of liability for contributory copyright infringement, several rules and doctrines preclude the availability of all the relief that the Plaintiffs seek.

1. The DMCA Safe Harbors Bar Damages and Most Injunctive Relief.

Plaintiffs ignore Cloudflare's safe harbors under the DMCA, which independently preclude monetary and (with limited exception) injunctive relief. 17 U.S.C. § 512.[6] Plaintiffs do

[5] Work-made-for-hire agreements and transfers of ownership must be in writing. 17 U.S.C. §§ 101 ("work made for hire"), 204(a) (transfers in writing). Plaintiffs rely on conclusory testimony that they own each image (*see* Dkt. 124-1 at 4 ¶ 7), but that is inadmissible—at least because it is improper opinion, violates the best evidence rule, and may not rest on personal knowledge (*see* Fed. R. Evid. 602, 701, 1002)—and does not satisfy their burden.

[6] While the DMCA supplies an additional reason Plaintiffs' claims fail, the Court does not have to

not dispute that Cloudflare qualifies as a service provider covered by the statute, § 512(k)(1); Bridges Decl. ¶ 8.c, Ex. 7, but they fail to address the safe harbors in their motion. Cloudflare qualifies for two distinct safe harbors under sections 512(a) and 512(b). 17 U.S.C. § 512(n).

a. Section 512(b) protects Cloudflare's caching.

Section 512(b) shields from liability a service provider's "intermediate and temporary storage" of material on its system or network, or system caching. This safe harbor recognizes that caching temporarily stores material that primarily resides elsewhere and that caches periodically update to mirror their sources. *See* Guinn Decl. ¶¶ 18–19. Cloudflare qualifies under section 512(b)(1) because it temporarily stores material that its customers make available online and transmits the material to visitors of its customers' websites who request the material. Guinn Decl. ¶ 23; Schonfeld Decl. ¶¶ 15, 36–49.

Cloudflare also meets the conditions of section 512(b)(2), which requires action in response to a valid notification of claimed infringement. *See* Paine Decl. ¶ 12. As Cloudflare explained above, a valid notification must state that the "originating site" of the material took down the material or that a court ordered it removed. § 512(b)(2)(E)(i), (ii). This is because removing material from a cache does *not* affect the originating site, but removing material from the origin will remove it from a cache. *See* Paine Decl. ¶ 12. Plaintiffs failed to comply with subsections (b)(2)(E)(i) and (ii). Paine Decl. ¶ 26. If Plaintiffs *had* sent a valid notification, Cloudflare has a system to respond expeditiously to remove the material. Paine Decl. ¶ 12. In fact, as a practical matter, the material likely would already be gone by the time Cloudflare responded because once the originating site takes down the material, Cloudflare's automated processes remove that material from Cloudflare's cache, generally within two hours. Guinn Decl. ¶ 24; Paine Decl. ¶ 12.

---

reach the statute's application to hold that Cloudflare is not subject to contributory infringement liability. *See* 17 U.S.C. § 512(l) (providing that even the failure to qualify for the DMCA's safe harbor "shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense").

b. Section 512(a) protects Cloudflare's transmissions.

Section 512(a) shields from liability a service provider's "transmission, routing, or providing of connections for digital online communications," also called a "conduit" function. § 512(k)(1)(A); *Ellison v. Robertson*, 357 F.3d 1072, 1081 (9th Cir. 2004). Cloudflare's core offering is a network that securely transmits and routes Internet communications at another's direction without modifying the content, § 512(k)(1)(A); Guinn ¶¶ 9–10; Schonfeld ¶ 23. Cloudflare meets each of the conditions for this safe harbor in subsection (a)(1) through (5). *See* Schonfeld Decl. ¶ 33. The Section 512(a) safe harbor for transmission services makes no provision for notifications of claimed infringement, because those services cannot remove any material from their transmissions.

Plaintiffs' proffered expert, Dr. Jonyer, does not dispute that Cloudflare meets the conditions of § 512(a)(1), (2), (3), and (5). Bridges Decl. ¶ 8.f, Ex. 7. He focuses instead on caching, specifically whether Cloudflare maintains a copy of material in cache "in a manner ordinarily accessible to anyone other than anticipated recipients" for longer than "reasonably necessary." § 512(a)(4). There is no competent evidence that it does, and instead Dr. Jonyer's opinion rests on a misinterpretation of the statute. Guinn ¶¶ 23–24; Schonfeld ¶¶ 25–27; *see Ellison*, 357 F.3d at 1081 (finding AOL's storage of the material for 14 days covered by 512(a)). But the Court need not address that issue, because Cloudflare's *caching* operations are covered by § 512(b). Apart from caching, Dr. Jonyer does not challenge Cloudflare's eligibility as a conduit service provider under section 512(a). Bridges ¶ 8.f, Ex. 7.

c. Cloudflare meets the conditions of section 512(i).

Cloudflare meets the two additional conditions for the safe harbors. *See* § 512(i)(1). *First*, Cloudflare adopted and informed its customers and others of its policy for termination in appropriate circumstances of repeat infringers, which it reasonably implements. Paine Decl. ¶¶ 20–24; *see Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109 (9th Cir. 2007). Plaintiff admits Cloudflare has "a repeat infringer policy" but falsely states it focuses "solely on subpoenas, court orders, and court adjudications." Dkt. 124-1 at 2; *see* Paine Decl. ¶¶ 20–23. Although Cloudflare's

policy prioritizes adjudicated findings of infringement (which is fully consistent with the provisions of § 512(b)(2)(E)), it also considers other objective indicia of validity and places less emphasis on mere unilateral allegations of infringement (which it reliably forwards to the hosting provider). Cloudflare's policy is consistent with the services it provides and sensitivities around removing security services, and it reflects the fact, discussed above, that terminating services will not prevent infringements. "[T]he statute permits service providers to implement a variety of procedures." *CCBill LLC*, 488 F.3d at 1109. The Ninth Circuit, for example, affirmed a summary judgment order finding that a website operator had satisfied this condition by implementing an unwritten policy that relied on "judgment, not a mechanical test, to terminate infringers based on the volume, history, severity, and intentions behind a user's infringing content uploads." *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 615–16 (9th Cir. 2018). Cloudflare's implementation is, likewise, reasonable. *See* Paine Decl. ¶¶ 21–23.

The Ninth Circuit also considers the copyright holder's compliance with notification requirements in evaluating the reasonableness of a defendant's policy implementation. *CCBill LLC*, 488 F.3d at 1111–12 (no genuine issue of material fact as to reasonable implementation since the plaintiff "did not provide notices that substantially complied with" the requirements). Here, Plaintiffs sent no valid notifications to Cloudflare[7] and Cloudflare thus had no obligation to apply a termination policy based on Plaintiffs' complaints. *See CCBill LLC*, 488 F.3d at 1111–12.

Second, Cloudflare accommodates, and does not interfere with, any "standard technical measures" that copyright owners use "to identify or protect copyrighted works." *See* § 512(i)(1)(B), (i)(2); Guinn Decl. ¶¶ 31, 33; *see* Paine Decl. ¶ 5. To the contrary, Cloudflare specifically designed its processes to get accurate, actionable information from complainants to its customers' hosts quickly, while also immediately giving complainants contact information for the hosting services so the complainants can contact the provider that can take down the material at

[7] *See above* Section III.A.2.*III.A.2.c* (discussing Plaintiffs' invalid notices under § 512(b)). Cloudflare's other safe harbor, section 512(a), does not provide for notifications because a transmission service like Cloudflare cannot remove or disable access to the material.

issue. Paine Decl. ¶¶ 5–16, Exs. 1–6. Cloudflare's safe harbor protection under section 512(a) and (b) precludes Plaintiffs from recovering damages or broad injunctive relief.

2. Plaintiffs Cannot Obtain Statutory Damages.

Plaintiffs have elected statutory damages. Bridges Decl. ¶ 26, Ex. 22; ¶ 27, Ex. 23. Plaintiffs' own evidence shows that they cannot satisfy the registration timing requirements to obtain statutory damages.[8]

First, Plaintiffs cannot recover based on registrations obtained after they filed this lawsuit. 17 U.S.C. § 411(a); *see Fourth Est. Pub. Benefit Corp. v. Wall-Street.com, LLC*, 139 S. Ct. 881, 886 (2019). Maggie Sottero submits with its motion two registration certificates dated 2019, *after* Plaintiffs sued Cloudflare (Dkt. 124-59 at MCMS 026979–81), and Plaintiffs have claimed others. *See* Bridges Decl. ¶ 20.c. Plaintiffs cannot assert those copyrights. *See Izmo, Inc. v. Roadster, Inc.*, No. 18-CV-06092-NC, 2019 WL 2359228, at *2 (N.D. Cal. June 4, 2019) (dismissing the plaintiff's claims for photographs it registered after it filed its original complaint).

As to the others, Plaintiffs must show they registered each copyright *before* alleged infringement began, unless infringement began after first publication, in which case Plaintiffs must have registered within three months of the publication. *See* 17 U.S.C. § 412. Almost all of Plaintiffs' registration certificates claimed published images. Dkts. 124-58; 124-59; Bridges Decl. ¶ 20.a. But Plaintiffs produced no admissible evidence of "publication" to make registrations within three months timely. And a number of certificates show copyrights registered more than three months after the claimed first publication. *See* Bridges Decl. ¶ 20.b. As to unpublished images, Plaintiffs have no competent evidence showing infringement began after registration. Bridges Decl. ¶ 7.a, Ex. 6; ¶ 24, Ex. 20; ¶ 25, Ex. 21. For these reasons, Plaintiffs cannot prove the

[8] Congress established a range of statutory damages "for all infringements involved in the action, with respect to *any one work*" and "*all the parts of a compilation or derivative work constitute one work*." 17 U.S.C. § 504(c)(1) (emphasis added). Each Plaintiff's images are parts of one compilation and derivative work, namely each Plaintiff's principal website. *See id.*; *see also* § 101; Dkt. 124-1 at 3–4 ¶¶ 4–5. Thus, Plaintiffs may, at most, calculate statutory damages for one work each. This issue will come to the fore if the Court does not grant summary judgment to Cloudflare.

timely registration requirements for statutory damages. *See* § 412(2); *Derek Andrew, Inc. v. Poof Apparel Corp*., 528 F.3d 696, 699–700 (9th Cir. 2008) (reversing award of statutory damages).

3. Plaintiffs Cannot Obtain a Permanent Injunction.

Besides their inability to recover any damages, Plaintiffs cannot obtain a permanent injunction because they cannot prove irreparable harm *from Cloudflare*. Generalized harm lacking a causal connection to the enjoined conduct does not justify an injunction. *See Perfect 10, Inc. v. Google, Inc*., 653 F.3d 976, 981–82 (9th Cir. 2011). Like Perfect 10, which had previously accused numerous companies of infringing its works, Plaintiffs have sought injunctive relief against many other online service providers. *See id.* at 982; Bridges Decl. ¶ 28, Ex. 24; ¶ 31, Ex. 27; ¶ 32, Ex. 28; ¶ 33, Ex. 29; ¶ 36, Ex. 32; ¶ 39, Ex. 35; ¶ 45, Ex. 41. Plaintiffs have secured injunctions against top-level domain registries, Internet search engines, payment processors, and other providers to take down websites, take control of domains, deindex websites from search engine results, and block money transfers. *See id*. They chose not to pursue that relief here and cannot show a causal connection between the harms they allege and *Cloudflare's* far more-removed services. An injunction against Cloudflare will not stop materials from appearing on customers' websites. Guinn Decl. ¶¶ 40–41. Nor have Plaintiffs shown any urgency seeking an injunction in this case. No injunction against Cloudflare is needed, or even appropriate, to prevent irreparable harm of infringements, because there is no evidence of harm *caused by Cloudflare*.

D. Plaintiffs' Failure to Prosecute the Direct Infringement Claim Against Doe Defendants Justifies Summary Judgment Against Plaintiffs on That Claim.

Plaintiffs move for summary judgment on their direct infringement claim, which they asserted against 500 "Doe" defendants, but they have never named those defendants, served them with process, or taken any other steps with the available information to pursue them.

The Ninth Circuit permits "Doe" nomenclature only until the close of discovery, and the plaintiff must obtain discovery to identify Doe defendants and amend the complaint to name them. *Gillespie v. Civiletti*, 629 F.2d 637, 642–43 (9th Cir. 1980); *Chenault v. San Ramon Police Dept.*, Case No. 15-cv-03662-SK, 2016 WL 4702653, at *2 (N.D. Cal. Sept. 8, 2016) (reviewing cases).

Cloudflare provided Plaintiffs contact information for both Doe defendants and their hosting providers. Bridges Decl. ¶ 21; ¶ 23.a, Ex 19. Perhaps fearing the consequences they faced before Judge Blakey, Plaintiffs never followed up on the information, never subpoenaed Does' hosting providers or email providers for more information, and never served the Does with process. Bridges Decl. ¶¶ 21–22.

Where a plaintiff moves for summary judgment against unnamed and unserved Doe defendants, courts in the Ninth Circuit grant summary judgment *to the Doe defendants*. *See, e.g.*, *Reed II v. Cox*, 821 F. App'x. 836, 836 (9th Cir. 2020) (affirming summary judgment against plaintiff who failed to identify Doe after nearly two years of discovery); *Chenault*, 2016 WL 4702653 at *3–4 (Doe defendants not identified and served). Plaintiffs failed to meet the requirements for even a default judgment, much less summary judgment. Consistent with Ninth Circuit authority, the Court should grand summary judgment *against Plaintiffs* on direct infringement.

IV. CONCLUSION

Because Cloudflare has not engaged in contributory infringement and Plaintiffs have no valid basis for remedies against it, Cloudflare is entitled to summary judgment. Plaintiffs' claims against the absent "Doe" defendants for direct infringement must fail because Plaintiffs never took any steps to prove a case against them. The Court should therefore deny Plaintiffs' motion in its entirety, grant Cloudflare's motion for summary judgment, and grant summary judgment to the Doe defendants as non-moving parties against Plaintiffs on their direct infringement claim.

V. OBJECTIONS TO EVIDENCE

A. Objections to Declaration of Markin (Dkt. 124-2)

Paragraphs 5–15 and Exhibits C–M incorporate entire transcripts of depositions of Plaintiffs' witnesses wholesale, regardless of relevance. The transcripts show motions to strike testimony as non-responsive or objections to direct examination by Plaintiffs' counsel, and Cloudflare incorporates here its objections and its motions to strike. Cloudflare additionally objects to the extent the evidence is inadmissible under F.R.E. 402, 403, 602, 701, 802, 901, and 1002.

Paragraphs 16–18 and 44 and Exhibits N–P and PP incorporate entire transcripts of depositions of Cloudflare-related witnesses. Cloudflare incorporates its objections at those depositions and additionally objects to the extent the testimony is inadmissible under F.R.E. 402, 403, 602, 802, 901, and 1002.

Paragraphs 19, 21–22, 33, 35, and 43, and Exhibits Q, S–T, EE, GG, and OO are inadmissible under F.R.E. 402, 403, 602, 802, 901, and 1002.

B. Objections to the Declarations of Taylor and Liney (Dkt. 124-50, 124-51)

Paragraphs 5–6 and the documents they refer to in both declarations are inadmissible under F.R.E. 602, 701, 802, 901, and 1002.

C. Objections to the Declaration of Ter-Saakov (Dkt. 125-52)

All references to "infringing," "infringements," or "Repeat Infringer Domains," and statements regarding XML Shop's system and technology, in Paragraphs 3–5, 7–12, and 14–17, and the Exhibits to which they refer are inadmissible under F.R.E. 402, 403, 602, 701, 702, and 1002.

Paragraphs 3–7, 9–12, and 15–17 and the exhibits to which they refer are inadmissible under F.R.E. 402, 403, 602, 701, and 1002 because they describe actions by persons other than Ter-Saakov (such as unnamed contractors overseas and Armen Petrossian), use "we" to obscure his lack of personal involvement and knowledge, involve subjects of expert knowledge as to which he has not been qualified or disclosed as an expert witness, and refer to processes and communications involving documents that are not in evidence.

Paragraph 13 and Exhibits D1 and D2 are inadmissible under F.R.E. 402.

Dated: June 23, 2021

FENWICK & WEST LLP

By: *Jedediah Wakefield*
Jedediah Wakefield

Attorneys for Defendant CLOUDFLARE, INC.