IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DISH NETWORK L.L.C., Plaintiff. v. DATACAMP LIMITED d/b/a CDN77 and DATAPACKET, Defendant.	Case No. 22-cv-00993 Judge John F. Kness

PLAINTIFF'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS

Defendant Datacamp Limited ("Datacamp")'s motion to dismiss for failure to state a claim (Doc. 20) should be denied because Plaintiff DISH Network L.L.C. ("DISH") adequately pleads claims against Datacamp for contributory and vicarious copyright infringement.

I. INTRODUCTION

For years Datacamp knowingly encouraged and assisted the Pirate Services to transmit DISH's copyrighted Works using the Datacamp CDN–despite Datacamp receiving more than 400 Infringement Notices asking it to stop or limit the Pirate Services' infringement. Datacamp knew the specific Pirate Services that were transmitting the Works and the specific URLs of those transmissions on the Datacamp CDN. Datacamp refused to take action against the Pirate Services because that would reduce Datacamp's profits–not only from the Pirate Services that were paying Datacamp to transmit the Works, but also from other pirate services that would no longer view the Datacamp CDN as a safe haven for infringement. Simply put, Datacamp prioritized its profits over its legal obligation to do what it could to prevent repeated infringement that it knew was occurring on the Datacamp CDN.

Datacamp's claim that DISH seeks to impose "unprecedented liability" is simply wrong. There is nothing unprecedented in holding Datacamp liable for the infringement taking place using the Datacamp CDN because Datacamp (1) encouraged or assisted the Pirate Services in known infringement and is liable as a contributory infringer and (2) profited from the Pirate Services' infringement while declining to stop or limit the infringement and is liable as a vicarious infringer. The Seventh Circuit and Supreme Court have held that secondary liability in these circumstances is appropriate and even necessary. *See, e.g.*, *In re Aimster*, 334 F.3d 643, 645-46, 654-55 (7th Cir. 2003); *Metro-Goldwyn-Mayer Studios Inc. v. Grokster*, 545 U.S. 913, 930 (2005) (commenting that contributory and vicarious copyright infringement is "well established in the law"). Indeed, Datacamp's liability under the facts alleged is so well-established that in 1998, Congress enacted the DMCA safe harbors in 17 U.S.C. § 512 to protect service providers from claims based on their users' copyright infringement but *only if* specified conditions are met such as terminating repeat infringers–something Datacamp refused to do. Contrary to Datacamp's framing of the dispute in the introduction to their motion, this case is "about actual wrongdoing on the part of Datacamp."

Datacamp does not challenge DISH's allegations that Datacamp encouraged or assisted the Pirate Services in their infringement, as required for Datacamp to be held a contributory infringer. Datacamp's argument that it lacked any knowledge of the Pirate Services' specific infringements is contrary to the well-pleaded allegations in DISH's complaint, including allegations of the more than 400 Infringement Notices that provided Datacamp knowledge of the Pirate Services' specific infringements and the acknowledgment of Datacamp's own CEO that it needed to be more strict with the Pirate Services because of the infringement that DISH reported. Datacamp's knowledge is sufficiently alleged and thus DISH's contributory infringement claim should not be dismissed.

Datacamp's argument that liability for vicarious infringement liability is improper is based

on the assumption that it lacked the ability to stop or limit the Pirate Services' infringement. But this assumption is contrary to DISH's allegations that Datacamp had several options available to prevent such infringement, ranging from termination of the Pirate Services' use of the Datacamp CDN, to disabling the transmissions of the Works, to geo-blocking those transmissions such that the Works were not publicly performed in the United States. Datacamp declined to take any of these steps to stop or limit the Pirate Services' infringement. Datacamp instead chose to profit from the infringement, charging the Pirate Services to transmit the Works based on the bandwidth consumed and keeping the Datacamp CDN a safe haven for infringement that drew in other pirate services. Datacamp's motion to dismiss DISH's vicarious infringement claim should be denied.

Finally, Datacamp's reliance on *Millennium Funding* only serves to establish that DISH's contributory and vicarious infringement claims are sound. Unlike Datacamp, the defendant that was dismissed in that case was two steps removed from the direct infringers, had no visibility to their infringements, and had no ability to stop or limit that infringement. Datacamp is more like the co-defendant held liable and ordered to pay nearly $10 million for contributory and vicarious infringement because that defendant, like Datacamp, had an immediate customer-relationship with the direct infringers, knew of their infringements based on notices of infringement it received, and was able to stop or limit the infringement by withholding or modifying the services it provided to the direct infringers. *Millennium Funding* further supports denial of Datacamp's motion to dismiss.

II. ARGUMENT

DISH's complaint need only set out "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The facial plausibility standard requires DISH to plead "factual content that allows the court to draw the reasonable inference that [Datacamp] is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)

(citing *Twombly*, 550 U.S. at 556). The factual allegations in DISH's complaint must be accepted as true and construed in the light most favorable to DISH. *Cheli v. Taylorville Cmty. Sch. Dist.*, 986 F.3d 1035, 1038 (7th Cir. 2021).

A. DISH Adequately Pleads Datacamp's Contributory Copyright Infringement.

The Seventh Circuit "prefer[s] the succinct definition of contributory infringement . . . : 'personal conduct that encourages or assists the infringement.'" *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 757 (7th Cir. 2012) (citation omitted). Datacamp does not dispute that DISH properly pleads the requisite conduct under *Flava*: Datacamp encouraged or assisted the Pirate Services to infringe DISH's exclusive right to publicly perform the Works by providing the Pirate Services with the Datacamp CDN, which was used to transmit the Works to users of the Pirate Services and which Datacamp made a safe haven for such infringement. (Mot. at 6-9; Compl. ¶¶ 25-62, 80.)

Rather, Datacamp argues that it cannot be held liable for contributory infringement because Datacamp purportedly was unaware of the Pirate Services' specific infringing conduct. (Mot. at 6-9.) Datacamp draws a line between general knowledge of infringement that takes place using the Datacamp CDN (which Datacamp admittedly had) and knowledge of the Pirate Services' specific infringements (which Datacamp denies knowing anything about). (*Id.*) Regardless of where the line is properly drawn,[1] Datacamp's motion to dismiss should be denied because DISH sufficiently pleads that Datacamp had knowledge of the Pirate Services' specific infringing conduct.

1. More Than 400 Infringement Notices Provided Datacamp Actual Knowledge Of The Pirate Services' Specific Infringements.

DISH adequately pleads that Datacamp had actual knowledge of specific infringements by the Pirate Services because Datacamp received more than 400 Infringement Notices that informed

[1]The Seventh Circuit observed that "it may be enough that the defendant *should* have known of the direct infringement." *Aimster*, 334 F.3d at 650.

Datacamp of such specific infringements. (Compl. ¶¶ 6-7, 52-55, 80.) Datacamp received further notice of the Pirate Services' infringement in the form of screenshots and network traffic logs that validated the infringement reported in the Infringement Notices. (*Id.* ¶¶ 55-56.) Indeed, knowledge of the Pirate Services' specific infringements went to the top of the Datacamp organization–CEO Zdenek Cendra acknowledged to DISH that Datacamp must be "more strict" with its customers to stop the infringement that DISH was reporting. (*Id.* ¶ 57.) Additionally, Datacamp was served with a court order that required Datacamp to disable the IP addresses that a Pirate Service was using to transmit content that infringed DISH's copyrights–but like the Infringement Notices themselves, Datacamp failed to comply with that order. (*Id.* ¶¶ 7, 24.)

These facts are more than sufficient to allege that Datacamp had knowledge of the Pirate Services' specific infringing activity. *See In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 650 (N.D. Ill. 2002) (finding notices of infringement, considered individually or collectively with other evidence, established defendant's knowledge to support contributory infringement); *Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2011 WL 1791557, at *4 (N.D. Ill. May 10, 2011) (denying motion to dismiss and finding seven notices of infringement combined with defendants' failure to prevent similar future infringing conduct sufficiently pleaded knowledge); *see also Sony Music Entm't v. Cox Commc'ns, Inc.*, 426 F. Supp. 3d 217, 231 (E.D. Va. 2019) (relying on infringement notices to grant summary judgment for plaintiff on the knowledge element of contributory infringement).

Datacamp's claim that the Infringement Notices are irrelevant in determining Datacamp's knowledge of the Pirate Services' infringements is based on a mischaracterization of *ALS Scan*. (Mot. at 7.) *ALS Scan* did not concern the defendant's knowledge of infringement; the issue was whether the defendant took simple measures to effectively stop known infringement and thus avoid liability for contributory infringement. *ALS Scan Inc. v. Steadfast Networks, LLC*, 819 F. App'x

522, 523-24 (9th Cir. 2020). The defendant established at summary judgment that it forwarded the notices of infringement to its customer and the infringing material was always removed. *Id.*at 523. The plaintiff argued that was not enough because the customer would likely continue to infringe. *Id.* at 524. The court agreed with the defendant and refused to impose contributory liability based on what a customer may do again, reasoning that "[t]he number of notices [defendant] previously received gives at most a general knowledge that infringement will likely occur again in the future; this does not give notice of any specific acts of infringement that are actually occurring." *Id.* (emphasis added). *ALS Scan* holds that liability for contributory infringement must be based on infringement that has actually taken place, rather than infringement that might occur in the future. DISH's contributory infringement claim is based on Datacamp encouraging and assisting the Pirate Services to publicly perform the Works–infringing conduct that actually occurred and not some speculative future infringement as in *ALS Scan*. (*See* Compl. ¶¶ 53, 79-80, Exs. 3-13.)

Furthermore, Datacamp cannot avoid liability like the defendant in *ALS Scan*, which took measures that effectively stopped the infringement, a critical finding made at summary judgment. 819 F. App'x at 523-24. Datacamp claims to have forwarded the Infringement Notices to the Pirate Services, but whether Datacamp actually forwarded them is a fact issue that cannot be resolved on DISH's complaint. (Compl. ¶ 55 [pleading only that Datacamp responded to *some* Infringement Notices "*saying* it had forwarded the notice"].) Even if Datacamp forwarded all the Infringement Notices, unlike in *ALS Scan*, the Pirate Services' infringement did not cease and Datacamp needed to implement measures to stop the infringement. (*Id.* ¶¶ 7, 24, 52-54, 80.) Datacamp failed to take measures to prevent infringement of DISH's copyrights. (*Id.* ¶¶ 4, 57, 81; *see* ¶¶ 58-62 [identifying simple measures that Datacamp refused to take].) Datacamp is subject to liability for contributory infringement where it had knowledge of the Pirate Services' specific infringements but, unlike the

defendant in *ALS Scan*, did nothing to effectively stop that infringement.[2]

2. Datacamp's Attempt To Hide Behind Its Own "Encryption" Requires Factual Findings Contrary To The Allegations In DISH's Complaint And Further Evidences Willful Blindness To The Pirate Services' Specific Infringements.

Datacamp goes well beyond the allegations in DISH's complaint by arguing that "it is not even possible for Datacamp to have . . . specific knowledge" of the Pirate Services' infringements because the "Pirate Services 'encrypt their streams.'" (Mot. at 7.) DISH pleads the Datacamp CDN is attractive to the Pirate Services because Datacamp provides the Pirate Services the ability to secure or "encrypt" their transmissions using security solutions provided by Datacamp. (Compl. ¶¶ 39-40; *see also* Mot. at 9 [referring to these security solutions as "[Datacamp's] encryption"].) Datacamp provides the Pirate Services this security in the form of a token-based access control feature that is part of the Datacamp CDN. (Compl. ¶¶ 32, 39-40.) These security solutions do not prevent Datacamp's access to and knowledge of the Works, but rather limit unauthorized access by users or other pirate services. (*Id.* ¶¶ 36, 39.) Indeed, Datacamp offered its customers like the Pirate Services "a clear picture of what's happening at each stage of the streaming pipeline" – the reasonable inference being that such information was equally available to Datacamp. (*Id.* ¶ 33; *see also* ¶¶ 26, 34, 37-38 [Datacamp offering to convert and transcode customer's video content, which also implies having the ability to access such content].)

Datacamp's argument that technical limitations prevented it from acquiring knowledge of the Pirate Services' infringement at best raises factual issues not properly resolved on the pleadings including: whether the Pirate Services' transmissions are secured at the point of entering into the

[2]Datacamp quotes *Torczon* stating "contributory copyright infringement cannot result 'merely based on a failure to take affirmative steps to prevent infringement,'" which further quoting *Torczon* means Datacamp must also "know or have reason to know of the allegedly infringing activity." (Mot. at 9.) *Pro Plans, Inc. v. Torczon*, No. 8:08cv136, 2010 WL 11523879, at *4 (D. Neb. Nov. 17, 2010). Datacamp's knowledge of the Pirate Services' specific infringing activity is adequately alleged. (Compl. ¶¶ 6-7, 24, 52-57, 80.)

Datacamp CDN; whether the transmissions are secured at all points while passing through the CDN; whether Datacamp could remove or bypass its own security solutions or otherwise access the content transmitted through its CDN; and whether Datacamp otherwise had knowledge of the infringement, for example based on information received from the Pirate Services such as content sources, stream names, or even responses to the claimed infringement. Datacamp's motion to dismiss is the not the proper vehicle to determine these factual issues. And, regardless of how these factual matters are resolved, Datacamp cannot ignore the more than 400 Infringement Notices that provided Datacamp knowledge of the Pirate Services' specific infringements.[3]

Likewise, Datacamp is not entitled to dismissal to the extent it claims to lack knowledge of the viewing habits of any particular users of the Pirate Services. (Mot. at 7 [arguing Datacamp cannot "view the data passing through the alleged Pirate Services to those companies' customers"]; *see also* 4 [arguing Datacamp has no access to "material displayed or viewed by end-users of its network"].) Not only does this argument present another factual issue outside the scope of a motion to dismiss, but the argument is irrelevant as Datacamp is not required to have knowledge of the users' viewing habits; rather, Datacamp's knowledge that the Pirate Services used the Datacamp CDN to transmit content infringing DISH's copyrights to such viewers–as made clear to Datacamp in the Infringement Notices–is sufficient for purposes of contributory infringement.

The *Millennium Funding* decisions that Datacamp relies on for its "encryption prevents knowledge" argument are of no help to Datacamp. (Mot. at 9, Exs. 1-2.) The defendant that moved

[3]In fact, in correspondence concerning Infringement Notices, Datacamp acknowledged that the token-based access control feature of the Datacamp CDN did not prevent Datacamp from accessing the Pirate Services' transmissions or identifying infringing content, such as Datacamp claiming "We do not have access nor can recognise what the content is exactly without a valid link" and "We do not need the token . . . . Links you provided in your last email are perfect. [W]e can now proceed with removal of the content." Datacamp had information needed to access and recognize the Pirate Services' transmissions of infringing content and the ability to stop or limit that infringement.

for dismissal (Quadranet) leased servers to its co-defendants (VPNs) that in turn provided VPN services to end users (the alleged direct infringers) accused of sharing copyrighted works using the BitTorrent protocol. *Millennium Funding, Inc. v. 1701 Mgmt. LLC*, 576 F. Supp. 3d 1192, 1212 (S.D. Fla. 2021). Quadranet–being two steps removed from the end users' infringement–was found to lack knowledge of specific infringing acts to support a contributory infringement claim, in part because the users' transmissions of copyrighted works were encrypted using the VPN's services. *Id.* at 1212-1213. The plaintiff failed to dispute Quadranet's argument that the VPN's encryption prevented Quadranet from having knowledge of infringements by the VPN's users. *Id.* Datacamp is not like Quadranet because (1) Datacamp's own customers, the Pirate Services (not end users of the Pirate Services), engaged in direct infringement and (2) Datacamp's own security solutions (not some security created by the Pirate Services) are claimed by Datacamp to prevent knowledge of such infringements. In short, Datacamp had the customer-relationship with the direct infringer and controlled the technology claimed to mask the infringement; Quadranet did not.

Datacamp is more like the VPN in *Millennium Funding*. After dismissing Quadranet, the court found that the complaint sufficiently stated a contributory infringement claim against a VPN defendant and granted default judgment, finding that the VPN's service (like the Datacamp CDN) contributed to the direct infringement and the VPN had knowledge of the infringement because of infringement notices it received (like the Infringement Notices received by Datacamp). *Millennium Funding, Inc. v. 1701 Mgmt. LLC*, No. 21-cv-20862, 2022 WL 901745, at *5 (S.D. Fla. Mar. 28, 2022). *Millennium Funding* supports the denial of Datacamp's motion to dismiss.[4]

[4]Datacamp's reliance on *Akanoc* is similarly misplaced because Datacamp is not like the defendant MSG that was two steps removed from the direct infringers and therefore found to have no reasonable means of withdrawing services to the direct infringers; rather, Datacamp is like the defendant Akanoc that provided servers and bandwidth to the direct infringers and was held liable for contributory infringement. (Mot. at 8.) *Louis Vuitton Malletier, S.A. v. Akanoc Sols., Inc.*, 658 F.3d 940, 942-44 (9th Cir. 2011).

As a final point, Datacamp's "encryption prevents knowledge" argument demonstrates that Datacamp willfully blinded itself to the Pirate Services' direct infringement. "Willful blindness is knowledge, in copyright law . . . as it is in the law generally." *Aimster*, 334 F.3d at 650. Datacamp "does not obtain immunity by using encryption [in the form of an access control feature] to shield itself from actual knowledge of the unlawful purposes for which the service is being used." *Id.* at 650-51. In fact, to the extent that Datacamp's own security solutions allegedly prevented it from having knowledge of the Pirate Services' infringement, this "is merely another piece of evidence that [Datacamp] was a contributory infringer." *Id.* at 655. Datacamp's argument that it lacked knowledge of specific infringements due to its own security solutions does not warrant dismissal.

DISH sufficiently states a claim for Datacamp's contributory copyright infringement.

B. DISH Adequately Pleads Datacamp's Vicarious Copyright Infringement.

Datacamp "infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." *Grokster*, 545 U.S. at 930. Datacamp is liable even if it "lacks knowledge of the infringement." *Id.* at 930 n.9; *see also Aimster*, 252 F. Supp. 2d at 654 ("[O]ne can be liable for vicarious copyright infringement even without knowledge of the infringement."). DISH sufficiently pleads Datacamp's vicarious copyright infringement.

1. Datacamp Profited From The Pirate Services' Infringement.

The profit element of vicarious copyright infringement is met by pleading "direct financial gain or that the 'availability of the infringing material acts as a draw for customers.'" *GC2 Inc. v. Int'l Game Tech. PLC*, 255 F. Supp. 3d 812, 825 (N.D. Ill. 2017) (citation omitted). The essential "'inquiry is whether there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits.'" *Id.* (citation omitted).

DISH adequately pleads that Datacamp experienced a direct financial gain from the Pirate Services' infringement. (Compl. ¶¶ 65-68, 75, 89.) Datacamp charged the Pirate Services based on the bandwidth they consumed using the Datacamp CDN. (*Id.* ¶¶ 68, 75.) The Pirate Services' transmission of the Works added to the amount of bandwidth used and in turn contributed to the amounts the Pirate Services paid to Datacamp. (*Id.*) Datacamp refused to take any measures to prevent the Pirate Services from infringing the Works because in doing so Datacamp would have reduced the Pirate Services' bandwidth consumption and therefore Datacamp's own profits. (*Id* ¶¶ 68, 75, 89.) Datacamp's argument that its bandwidth charges did not depend on the type of content the Pirate Services transmitted (infringing versus non-infringing) misses the mark: DISH pleads that the Pirate Services' transmission of the Works used bandwidth and thus added to the amounts the Pirate Services paid to Datacamp. (*Id.*; Mot. at 12-13.) DISH sufficiently alleges that Datacamp received a direct financial benefit from the Pirate Services' infringement. *Aimster*, 252 F. Supp. 2d at 655 (finding direct infringers' payment to defendant for use of platform where infringement occurred was "without question" a direct financial benefit for purposes of vicarious infringement); *GC2*, 255 F. Supp. 3d at 825 (denying motion to dismiss and finding financial benefit sufficiently alleged based on direct infringers' payments to defendants).

DISH also adequately pleads that the ongoing availability of the Works that resulted from Datacamp's failure to take appropriate action against the Pirate Services acted as a draw for those Pirate Services to remain paying customers of Datacamp and attracted other pirate services to the Datacamp CDN. (Compl. ¶¶ 4-5, 64-66, 88-89.) At least eleven Pirate Services used the Datacamp CDN to infringe DISH's copyrights across a span of, at minimum, nearly four years. (*Id.* ¶¶ 6, 53.) Pirate Services became customers of the Datacamp CDN because of Datacamp's lax infringement policy, resulting in payments to Datacamp. (*Id.* ¶¶ 65-66, 88-89.) For this additional reason, DISH

adequately pleads that Datacamp profited from the Pirate Services' infringement. *Aimster*, 252 F. Supp. 2d at 655 (finding "the existence of infringing activities" was a draw for users of defendants' service and this satisfied the financial benefit element of vicarious infringement); *see also Flava*, 2011 WL 1791557, at *5 (rejecting argument that plaintiff must plead the defendant gained or lost customers due to the presence or absence of infringing material because such a standard was "overlydemanding" and not supported by law; "[a]ll plaintiff need allege is that the availability of infringing material . . . is a draw for customers"); *UMG Recordings, Inc. v. RCN Telecom Servs., LLC*, No. 191272 (MAS) (ZNQ), 2020 WL 5204067, at *12 (D.N.J. Aug. 31, 2020) (denying motion to dismiss and finding allegations that defendant ISP failed to police infringing users and in turn attracted more users pleaded a financial benefit for vicarious infringement claim).[5]

Datacamp's reliance on the dismissal of a vicarious copyright infringement claim against Quadranet in *Millennium Funding* is misplaced because Datacamp is not like Quadranet. (Mot. at 13.) Quadranet was paid by its customers, the VPNs, and not the users alleged to have engaged in the direct infringement; therefore, the court held that Quadranet did not directly benefit from that infringement. 576 F. Supp. 3d at 1214-15. Unlike Quadranet, Datacamp is not only paid by the Pirate Services that engaged in direct infringement, but the Pirate Services' payments to Datacamp are tied to the infringement of the Works. (Compl. ¶¶ 68, 75.) Datacamp is more like the VPN in *Millennium Funding* that was found to have profited from its customers' infringement and thus

[5]The *Grande* case relied on by Datacamp uses the overly demanding standard this District rejected in *Flava*; however, DISH satisfies that heightened standard as Datacamp is alleged to have gained customers because of Datacamp's failure to terminate infringers such as the Pirate Services. (Mot. at 12; Compl. ¶¶ 4-5, 64-66, 88-89.) *Grande* made other findings that are contrary to Datacamp's arguments, for example holding that infringement notices are properly considered in finding knowledge for contributory infringement and that terminating services is an appropriate measure to deal with direct infringers. *See UMG Recordings, Inc. v. Grande Commc'ns Networks, LLC*, 384 F. Supp. 3d 743, 768 (W.D. Tex. 2019).

held liable for vicarious infringement. 2022 WL 901745, at *5.[6]

2. Datacamp Declined To Stop Or Limit The Pirate Services' Infringement.

The second requirement for vicarious infringement is met by pleading Datacamp's "right and ability" to stop or limit the Pirate Services' direct infringement. *Grokster*, 543 U.S. at 930 n.9. Datacamp does not dispute having the *right* to stop or limit the Pirate Services' direct infringement. (Mot. at 10-11; Compl. ¶ 64 [pleading Datacamp's contractual relationship with the Pirate Services provided Datacamp the right to terminate for any reason].) Datacamp's argument that it lacked the *ability* to stop or limit the Pirate Services' infringement fails for several reasons.

Datacamp had the ability to terminate the Pirate Services' use of the Datacamp CDN, which would have stopped or limited the transmission of the Works using the Datacamp CDN. (Compl. ¶ 63.) *See Aimster*, 252 F. Supp. 2d at 654-55 (finding defendant could stop or limit infringement because it could terminate direct infringer and control access to infringing material on its platform); *GC2*, 255 F. Supp. 3d at 824 (finding ability to stop or limit infringement adequately pleaded based on allegations that defendant could terminate its relationship with direct infringer). Datacamp's argument–that terminating the services it provides to a direct infringer, like the Pirate Services, is too harsh–cannot be reconciled with the case law and at best presents a question of fact outside the scope of a motion to dismiss.[7] Indeed, in circumstances involving repeat infringers as alleged here,

[6]The *Veoh* case cited by Datacamp involved a vicarious infringement claim against *investors* of a business alleged to profit from direct infringement by attracting new users and advertisers. (Mot. at 12.) The court found the plaintiff failed to plead that the investors, unlike the business itself, profited. *UMG Recordings, Inc. v. Veoh Networks, Inc.*, No. CV 07-5744 AHM (AJWx), 2009 WL 334022, at *6 (C.D. Cal. Feb. 2, 2009). DISH does not assert claims against Datacamp's investors; rather, DISH's vicarious infringement claim is against Datacamp–the direct recipient of the Pirate Services' payments.

[7]Datacamp's carrot and stick analogy from *Visa* is inapplicable because, unlike Visa that merely processed payments for an infringer and thus provided the infringer only a financial carrot, Datacamp held the stick to stop or limit the Pirate Services' infringement by terminating or restricting their use of the Datacamp CDN, but Datacamp refused to act and profited from the infringement. (Mot. at 11; Compl. ¶¶ 63-64, 67.)

the DMCA requires service providers to terminate infringers to maintain defenses to infringement claims brought against the service providers. 17 U.S.C. § 512(i)(1)(A). Datacamp is not eligible for any DMCA safe harbor for several reasons. (Compl. ¶¶ 70-75.) The point is that Datacamp is wrong to suggest that, as a matter of law, account termination is an unreasonable measure to stop the Pirate Services' infringement through the Datacamp CDN.

Moreover, Datacamp had the ability to stop or limit the Pirate Services' direct infringement by means short of terminating them, such as by disabling transmissions only of the Works (while leaving other transmissions by the Pirate Services active) or by geo-blocking the Pirate Services' transmissions of the Works to prevent the public performance of the Works in the United States (leaving the Pirate Services free to make transmissions that do not infringe DISH's rights). (Compl. ¶¶ 57, 63, 68.) The *Millennium Funding* and *Venus Fashions* cases relied on by Datacamp found similar measures sufficient to stop or limit infringement. *Millennium Funding*, 2022 WL 901745, at *5 (finding VPN could stop direct infringement by customers using VPN's servers, such as by null-routing customers' IP addresses); *Venus Fashions, Inc. v. ContextLogic, Inc.*, No. 3:16-cv-907-J-39MCR, 2017 WL 2901695, at *25 (M.D. Fla. Jan. 17, 2017) (finding defendant could stop or limit infringement by taking down infringing content).[8] Datacamp's arguments against disabling or geo-blocking the Pirate Services' transmissions of the Works–claiming that such measures are impossible and too tough on direct infringers–are contrary to the allegations in DISH's complaint and highly suspect given Datacamp's end-to-end control over its CDN, and in any event are factual in nature and thus not properly resolved on a motion to dismiss. (Compl. ¶¶ 25-51.)

[8]Datacamp's reliance on *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001), is misplaced because that case did not address vicarious infringement but rather DMCA safe harbor ineligibility, which according to the Ninth Circuit requires "something more" in terms of an ability to stop or limit infringing activity than is required to impose liability for vicarious infringement. (Mot. at 11.) *See, e.g.*, *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013).

DISH sufficiently states a claim for Datacamp's vicarious copyright infringement.

III. CONCLUSION

DISH adequately pleads claims against Datacamp for contributory and vicarious copyright infringement. Datacamp provided the Pirate Services with the Datacamp CDN knowing the Pirate Services were using the Datacamp CDN to infringe DISH's copyrights as made clear to Datacamp in more than 400 Infringement Notices informing Datacamp in detail of the specific infringements. Datacamp refused to take any action to stop or limit the Pirate Services' infringement taking place on the Datacamp CDN, prioritizing its own profits over its legal obligations. Had Datacamp acted differently and policed infringement on the Datacamp CDN rather than making it a safe haven for infringement–as most businesses referenced in Datacamp's closing footnote do on their platforms–this lawsuit might have been avoided. Datacamp's motion to dismiss should be denied.

Dated: September 2, 2022.

/s/ Timothy M. Frank
Timothy M. Frank (*pro hac vice*)
HAGAN NOLL & BOYLE, LLC
820 Gessner, Suite 940
Houston, Texas 77024
Tel: (713) 343-0478
Fax: (713) 758-0146
timothy.frank@hnbllc.com

David M. Lewin
LEWIN VERVENIOTIS LAW GROUP
175 W. Jackson Boulevard, Suite 1600
Chicago, Illinois 60604
Tel: (312) 540-7556
Fax: (312) 540-0578
dml@lewver.com

Counsel for Plaintiff DISH Network L.L.C.