

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

DISH NETWORK LLC,

Plaintiff,

v.

DATA CAMP LIMITED,

Defendant.

No. 22-cv-00993

Judge John F. Kness

**MEMORANDUM OPINION & ORDER**

Plaintiff Dish Network LLC brings suit against Defendant Datacamp Limited for contributory and vicarious copyright infringement. Defendant has moved to dismiss both counts under Rule 12(b)(6) of the Federal Rules of Civil Procedure, arguing that the allegations in the complaint fail to state a claim. For the following reasons, Defendant’s motion is denied.

**I. BACKGROUND**

Plaintiff is the fourth-largest pay-tv provider in the United States, offering more than 400 domestic and international television channels in 27 languages to millions of subscribers nationwide. (Dkt. 1 ¶ 1.) Plaintiff contracts for and licenses the exclusive right to distribute and publicly broadcast these television channels (the “Protected Channels”) and their respective copyrighted programming (the “Works”). (*Id.* ¶¶ 18–20.) Illegal streaming services (the “Pirate Services”), however, capture the Works aired on the Protected Channels and transmit them over the internet to

viewers in the United States who pay a fee to view the content. (*Id.* ¶ 21.) The Pirate Services’ fee is a fraction of Plaintiff’s because the Pirate Services do not pay any fees to license the content they deliver. (*Id.* ¶ 2.)

These Pirate Services often rely on third-party content delivery networks (CDNs) to deliver content to their customers, including Defendant’s CDN. (*Id.* ¶¶ 3, 25.) A CDN is a “geographically distributed network of datacenters and computer servers designed to transmit content over the internet with high efficiency and peak performance.” (*Id.* ¶ 25.) Defendant’s CDN “encod[es] Protected Channel feeds into signals capable of being transmitted efficiently over a CDN” and “secur[es] the transmissions to make them accessible only to individuals permitted by the Pirate Services.” (*Id.* ¶ 36.) To facilitate a user-friendly streaming experience, Defendant’s CDN addresses issues concerning “latency; scalability and redundancy; smooth performance, security; and savings.” (*Id.* ¶ 28–33.) Simply put, Defendant’s CDN is a network of servers that facilitates internet streaming to the users. (*Id.* ¶ 27.) Pirate Services pay Defendant for CDN access based on the amount of CDN bandwidth they use, and the bandwidth consumed is in part a function of the number of end users. (*Id.* ¶¶ 66, 68.)

Plaintiff has tried to stop the Pirate Services’ continued copyright infringement. Plaintiff sent Defendant over 400 infringement notices under the Digital Millennium Copyright Act (“DMCA”) requesting that Defendant remove the infringing content, but Defendant failed to terminate the Pirate Services access to the CDN. (*Id.* ¶ 6.) Plaintiff also filed lawsuits and obtained judgments against

several of the Pirate Services. (*Id.* ¶ 7.) A court order from at least one of these lawsuits required Defendant to disable all IP addresses used by that Pirate Service to transmit the infringing works, but Defendant failed to promptly disable the IP addresses. (*Id.*)

Because Pirate Services utilizing Defendant’s CDN continue to infringe Plaintiff’s copyrights in the Works, Plaintiff sued Defendant for contributory and vicarious copyright infringement under 17 U.S.C. § 501. (*Id.* ¶¶ 76–91.) Because Defendant has “ignore[ed] or turn[ed] a blind eye to the Pirate Services’ willful and repeated infringement” despite having knowledge of the Pirate Services’ infringement and the ability to prevent it, Plaintiff alleges that Defendant is contributorily liable for copyright infringement. (*Id.* ¶¶ 80–82.) Defendant is also vicariously liable, according to Plaintiff, because Defendant directly profited from the Pirate Services’ infringement while having the right and ability to prevent the infringement. (*Id.* ¶¶ 87–89.) Defendant moved to dismiss both counts for failure to state a claim under Rule 12(b)(6) of the Federal Rules of Civil Procedure. (Dkt. 20.)

## II. LEGAL STANDARD

A motion under Rule 12(b)(6) “challenges the sufficiency of the complaint to state a claim upon which relief may be granted.” *Hallinan v. Fraternal Ord. of Police of Chi. Lodge No. 7*, 570 F.3d 811, 820 (7th Cir. 2009). Each complaint “must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). These allegations “must be enough to raise a

right to relief above the speculative level.” *Twombly*, 550 U.S. at 555. Put another way, the complaint must present a “short, plain, and plausible factual narrative that conveys a story that holds together.” *Kaminski v. Elite Staffing, Inc.*, 23 F.4th 774, 777 (7th Cir. 2022) (cleaned up). In evaluating a motion to dismiss, the Court must accept as true the complaint’s factual allegations and draw reasonable inferences in the plaintiff’s favor. *Iqbal*, 556 U.S. at 678. But even though factual allegations are entitled to the assumption of truth, mere legal conclusions are not. *Id.* at 678-79.

### III. DISCUSSION

#### A. Contributory Infringement

A defendant is liable for contributory copyright infringement when it, “with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.” *Myers v. Harold*, 279 F. Supp. 3d 778, 796 (N.D. Ill. 2017) (citation omitted). A party acts with knowledge where it “has been notified of specific infringing uses of its technology and fails to act to prevent future infringing uses, or willfully blinds itself to such infringing uses.” *Flava Works, Inc. v. Gunter*, 2011 WL 1791557, at \*4 (N.D. Ill. May 10, 2011); *see also ALS Scan, Inc. v. Steadfast Networks, LLC*, 819 F. App’x 522, 524 (9th Cir. 2020) (defendant must have “notice of [] specific acts of infringement that are actually occurring” rather than “general knowledge that infringement will likely occur again in the future”).

Plaintiff alleges that Defendant knew of specific infringing uses of its CDN because Plaintiff sent Defendant over 400 DMCA infringement notices specifying the name of the Pirate Service, the Protected Channel, and the associated “IP addresses,

domain names, and the URLs used to transmit the Works.” (Dkt. 1 ¶ 53–54; Dkt. 1-1.) Plaintiff also supplemented its infringement notices by providing “screenshots of transmissions of the Works and network traffic recorded in the form of PCAP files,<sup>1</sup> showing that [Defendant’s] servers were responsible for the infringing transmissions on the Pirate Services.” (*Id.* ¶ 56.) In its complaint, Plaintiff provides a screenshot of a sample PCAP file sent to Defendant, which appears to contain IP addresses and URLs. (*Id.*) Defendant, however, contends that the infringement notices fail to establish that Defendant knew of specific infringing uses. (Dkt. 21, at 7.) According to Defendant, infringement notices give at most a “general knowledge” that future infringement is likely, meaning Defendant had no duty to prevent infringement. (*Id.*)

The “specific infringing use” standard “focuses on a defendant’s ability to act upon the information provided.” *Sony Music Entm’t v. Cox Commc’ns, Inc.*, 426 F. Supp. 3d 217, 233 (E.D. Va. 2019). Infringement notices must therefore alert the defendant as to which copyrighted material is being infringed and which users are doing the infringing. *Id.*; see *Perfect 10, Inc v. Amazon.com, Inc.*, 508 F.3d 1146, 1172 (9th Cir. 2007) (infringement notices, if adequately detailed, would establish defendant’s knowledge). For instance, *In re Aimster* held that the defendant, which ran a peer-to-peer file sharing program, had the requisite knowledge when plaintiffs sent notices containing screenshots of defendant’s “system showing the availability

---

<sup>1</sup> “PCAP” is short for “Packet Capture,” a file format used by computer programs that “allows a user to record data transmission across computer networks by capturing data in a file.” *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2019 WL 4727537, at \*5 (S.D.N.Y. Sept. 26, 2019).

of Plaintiffs’ copyrighted sound recordings on [specific] users’ hard drives.” 252 F. Supp. 2d 634, 650 (N.D. Ill. 2002). And in *Flava Works, Inc. v. Gunter*, the court held that the plaintiff stated a claim for contributory infringement by alleging that the defendant failed to act after receiving DMCA notices “identify[ing] specific infringing files and users as well as specific repeat infringers.” 2011 WL 1791557, at \*4 (N.D. Ill. May 10, 2011).

Plaintiff forwarded hundreds of infringement notices containing ample information that would have allowed Defendant to prevent infringement. The notices named the Pirate Service, the infringing Works being broadcasted, and the IP addresses, URLs, and domain names being used to transmit the infringing works. This information provided Defendant with sufficient knowledge to act against the infringing Pirate Services—in other words, with knowledge of specific infringing uses. *In re Aimster*, 252 F. Supp. 2d at 650; *Flava Works*, 2011 WL 1791557, at \*4.

Defendant principally relies on *ALS Scan* for the proposition that “notices . . . give[] at most a general knowledge that infringement will likely occur again in the future” but do “not give notice of any specific acts of infringement that are actually occurring.” 819 F. App’x at 524. *ALS Scan* is distinguishable, however, because the defendant forwarded the infringement notices to the infringing parties who subsequently removed the infringing materials. *Id.* at 523. Still unsatisfied, the plaintiff complained that the defendant should have taken further remedial actions because the infringing parties might resume their infringement. *Id.* at 523–24. The Ninth Circuit rejected plaintiff’s argument because the infringement had ceased, and

liability cannot be imposed by speculating on the likelihood of future infringement based on past infringement notices. *Id.* at 524.

Conversely here, Defendant received infringement notices but did not take sufficient actions to remove the infringing material.<sup>2</sup> The Pirate Services documented in the infringement notices have infringed and continue to infringe Plaintiff's copyrights. Further, unlike in *ALS Scan*, Plaintiff uses the infringement notices to impute knowledge to Defendant about past and present infringement, not speculative future infringement.

Moreover, the infringement notices are not the only evidence of Defendant's knowledge. The complaint alleges that Plaintiff served Defendant with a court order requiring Defendant to disable IP addresses associated with certain Pirate Services, yet Defendant failed to do so promptly. (Dkt. 1 ¶¶ 7, 24.) Defendant's CEO also allegedly "acknowledged in September 2019 that Datacamp needed to be 'more strict' with its customers and that 'cooperation with the customer is not the good way' to stop the infringement." (*Id.* ¶ 57.) These allegations, taken together with the over 400 infringement notices documenting "specific acts of infringement that are actually

---

<sup>2</sup> Defendant argues that it forwarded the infringement notices to the Pirate Services to remove the infringing content (Dkt. 21, at 8), but Plaintiff contends that whether Defendant "actually forwarded them is a fact issue that cannot be resolved on [Plaintiff's] complaint." (Dkt. 36, at 6.) This factual issue cannot be resolved at this stage because the complaint alleges that Defendant, upon receiving the infringement notices, "failed to respond, responded by saying it had forwarded the notice to the responsible customer to remove the infringing content, or asked for additional information." (Dkt. 1 ¶ 55.) In other words, Plaintiff alleges that Defendant forwarded *some* infringement notices, but it is not clear how many. In any event, the Pirate Services continued to infringe after Defendant received the notices, meaning Defendant's actions failed to prevent the infringement.

occurring,” *ALS Scan*, 819 F. App’x at 524, establish Defendant’s knowledge of specific infringing uses of its CDN.<sup>3</sup> Accordingly, Defendant’s motion to dismiss Plaintiff’s claim for contributory infringement is denied.<sup>4</sup>

## **B. Vicarious Infringement**

To state a claim for vicarious copyright infringement, a plaintiff must establish that the defendant has “(1) the right and ability to supervise the infringing conduct and (2) a direct financial interest in the infringing activity.” *GC2 Inc. v. Int’l Game Tech. PLC*, 255 F. Supp. 3d 812, 824 (N.D. Ill. 2017) (quoting *Perfect 10, Inc. v. Giganeews, Inc.*, 847 F.3d 657, 673 (9th Cir. 2017)). Defendant argues that the

---

<sup>3</sup> Defendant argues that knowledge of infringement cannot be imputed based on Defendant’s failure to remove or disable access to the Pirate Services after receiving the infringement notices because “copyright infringement liability cannot be found ‘merely based on a failure to take affirmative steps to prevent infringement.’” (Dkt. 21, at 7 (quoting *Plan Pros v. Torczon*, 2010 WL 11523879, \*4 (D. Neb. Nov. 17, 2010)).) *Torczon* held that the defendants could not be liable *solely* based on the failure to take affirmative steps to prevent infringement because neither defendant “knew or had reason to know of the allegedly infringing activity.” *Id.* at \*5. Here, Defendant had actual knowledge because of the infringement notices.

<sup>4</sup> Defendant argues that it is impossible for it to have knowledge of specific infringing uses because the CDN encrypts the Pirate Services’ streams, preventing Defendant from accessing the content. (Dkt. 21, at 7.) Even if encryption prevented Defendant from viewing the infringing materials, the infringement notices provided Defendant with knowledge. Ignoring the infringement notices, the Court would still reject Defendant’s encryption argument. Defendant relies primarily on *Millennium Funding, Inc. v. 1701 Management LLC*, 576 F. Supp. 3d 1192 (S.D. Fla. 2021). In *Millennium Funding*, the court held that Quadranet, who provides server space to VPN companies, who in turn encrypt their customers’ infringing activity, did not have the requisite knowledge. *Id.* at 1212–13. But *Millennium Funding* is distinguishable because Defendant is more akin to the VPN companies, not Quadranet. Like the VPN companies, Defendant performs the encryption for its infringing customers. Quadranet, in contrast, did not perform the encryption nor deal directly with the infringing party. Instead, Quadranet’s customers—the VPN companies—intermediated Quadranet’s legitimate activities from the infringing activities. In addition, it is “disingenuous of Defendant[] to suggest that [it] lack[s] the requisite level of knowledge when [its] putative ignorance is due entirely to an encryption scheme that [it] put in place [itself].” *In re Aimster*, 252 F. Supp. 2d at 651.



allegations in the complaint fail to establish either requirement.

**i. Right and Ability to Supervise**

Plaintiff alleges that Defendant had the ability to stop or limit the Pirate Services' infringement because it could have terminated the Pirate Services' access to Defendant's CDN for "any reason" under Defendant's service agreement.<sup>5</sup> (Dkt. 1 ¶ 64.) Short of terminating access to the CDN, Plaintiff says that Defendant could have required the Pirate Services to verify their rights in the Works before broadcasting, investigated compliance with the infringement notices more thoroughly, implemented a multi-strike policy, or employed geoblocking to prevent broadcasting of the Works in the United States. (*Id.* ¶¶ 58–63.) Defendant, however, contends that Plaintiff's suggestions for controlling infringement were "either impossible or far too overbroad." (Dkt. 21, at 10–11.)

Courts must examine "the system's current architecture" to "determine whether a defendant has the capacity to halt infringement." *Venus Fashions v. ContextLogic, Inc.*, 2017 WL 2901695, at \*25 (M.D. Fla. Jan. 17, 2017). When the defendant can terminate its users' access to the system to prevent infringement, the defendant has the ability to stop infringement. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001) ("The ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise."); *Perfect 10, Inc.*, 508 F.3d at 1174 ("Because Napster . . . could

---

<sup>5</sup> Because the complaint alleges that Defendant's service agreement permitted Defendant to terminate its customers' access to the CDN for any reason, Defendant does not argue that it lacked the "right" to supervise the infringing conduct. Defendant contends solely that it lacked the "ability" to supervise.

terminate its users' accounts and block their access to the Napster system, Napster had the right and ability to prevent its users from engaging in the infringing activity."); *In re Aimster*, 252 F. Supp. 2d at 655 (Defendants have the right and ability to supervise because defendants "have the right to terminate individual users" and "control the access of Aimster's users" through a log-in feature.).

None of the cases cited by Defendant refute this proposition. Defendant relies on *Venus Fashions*, but that case addressed whether the defendant could utilize a "fingerprinting" system to prevent infringement. 2017 WL 2901695, at \*12, 25. It did not address whether terminating an infringing user's access was an "overbroad" remedy. *Id.* Defendant also cites *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093–94 (C.D. Cal. 2001). This case also did not address whether terminating access is an overbroad remedy; instead, it analyzed whether the defendant *could* in fact terminate such access. *Hendrickson* held that eBay had no ability to stop the infringing activity—the sale of infringing goods—because "eBay has no involvement in the final exchange and generally has no knowledge whether a sale is actually completed." *Id.* at 1094. Lastly, Defendant relies on *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 805 (9th Cir. 2007). *Visa* held that the defendant, a payment processor, did not have the right and ability to control infringement even though the defendant "could likely take certain steps," such as refusing to process infringing transactions, "that may have the indirect effect of reducing infringing activity on the internet at large." *Id.* at 803. Unlike a payment processor, Defendant could do more than have an indirect effect: Defendant could directly stop the infringement by

terminating access to the CDN.

In sum, the complaint alleges that Defendant received numerous notices identifying the infringing Pirate Services and that Defendant had the ability to terminate their access to the CDN. *In re Aimster*, 252 F. Supp. 2d at 655 (ability to control access to system means defendant had right and ability to supervise). None of the authorities cited by Defendant support the proposition that terminating access is an overbroad remedy. Accordingly, the Court need not consider Plaintiff's alternative proposed remedies. The complaint adequately alleges that Defendant had the ability to stop the infringement.

**ii. Direct Financial Interest**

Plaintiff contends that Defendant has a direct financial interest in the Pirate Services' infringement because the infringement is a draw for customers. The infringement—unauthorized production of the popular Protected Channels and Works at an artificially low price—increases the number of end users of the Pirate Services, which increases the Pirate Services' bandwidth usage and consequently the payments made to Defendant. (Dkt. 1 ¶¶ 66, 68.) Moreover, the Pirate Services are motivated to sign up and remain with Defendant's CDN because of Defendant's lax policy towards infringement, which also increases overall bandwidth consumption. Defendant argues, however, that “attracting users” and “increasing the value of its business” are “too far removed from the alleged infringement to be considered a ‘direct’ financial interest.” (Dkt. 21 at 12 (quoting *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 2009 WL 334022, at \*6 (C.D. Cal. Feb. 2, 2009)).)

The financial benefit requirement is satisfied “where there is evidence of a direct financial gain or that the ‘availability of infringing material acts as a draw for customers.’” *GC2 Inc.*, 255 F. Supp. 3d at 825 (quoting *Ellison v. Robertson*, 357 F.3d 1072, 1078 (9th Cir. 2004)). The infringing material need only be a “contributing factor” to a “consumer’s decision to purchase a product or service.” *Id.* 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 that benefit is.” *Id.* (quoting *Ellison*, 357 F.3d at 1079).

Applying these principles, many courts have held that internet services have a direct financial interest when the infringing material induces customers to purchase the service. In *GC2*, the court held that the defendant, which advertised and sold computer games over the internet using infringing artwork, had a direct financial interest because the artwork “gain[ed] the interest of consumers.” *GC2 Inc.*, 255 F. Supp. 3d at 825. And *Flava Works* and *Aimster* both held that infringement that induces customers to subscribe to the defendant’s service satisfies the direct financial gain requirement. *Flava Works*, 2011 WL 1791557, at \*5 (“All plaintiff need allege is that the availability of infringing material on myVidster is a draw for customers.”); *In re Aimster*, 252 F. Supp. 2d at 655 (“Financial benefit element is [] satisfied where, as here, the existence of infringing activities acts as a draw for potential customers” and those customers “must pay \$4.95 per month to use the service.”); see *Coach, Inc v. Swap Shop, Inc.*, 916 F. Supp. 2d 1271, 1282 (S.D. Fla. 2012) (Operators of flea market obtained direct financial benefit by collecting “rents

from their vendors, including those selling fake Coach products, . . . which are fueled in large part by the draw created by the widespread availability of fake Coach products.”).

Defendant relies on *UMG Recordings* to argue that attracting customers is not a direct financial interest. 2009 WL 334022, at \*6. *UMG Recordings* held that a business’s investors did not obtain a direct financial benefit even though the business gained customers from infringement because the investors would only “profit from their investments through the sale of [the business] to a potential acquiring company.” *Id.* The complaint, however, did “not allege that the investors received, or will receive, fees paid by customers.” *Id.* The potential sale, standing alone, was “too far removed from the alleged infringement” to be a direct financial interest. *Id.* Unlike the investors in *UMG Recordings*, who would only benefit from a future sale, Defendant here directly realized a financial gain from the infringement because payments from the Pirate Services increased as customers were attracted and consumed more bandwidth.

Defendant also cites to *Millennium Funding, Inc. v. 1701 Management LLC*, 576 F. Supp. 3d 1192, 1214–15 (S.D. Fla. 2021). The defendant, Quadranet, provided server space to VPN companies, who in turn were paid by users that engaged in infringing activity. *Id.* at 1214. The Court held that Quadranet did not receive a direct financial benefit because Quadranet was “paid by the VPN companies, not the end users of the VPN companies who engaged in the infringing activity,” and “Quadranet was paid by the VPN companies regardless of whether the end users engaged in

infringing activities.” *Id.* at 1214–15. Unlike Quadranet, Defendant here is paid directly by the infringing parties, the Pirate Services. Moreover, the payment Defendant receives is dependent on infringement because Defendant is paid based on bandwidth, and the infringement induces end users to consumer more bandwidth.


In view of the cases discussed, Defendant obtained a direct financial benefit. The complaint’s allegations establish a “causal relationship” between infringement and profit. *GC2 Inc.*, 255 F. Supp. 3d at 825. The Protected Channels and Works attract end users to the Pirate Services, which increases bandwidth consumption and the payments made to Defendant. The profits reaped from infringement also attracts new Pirate Services to Defendant’s CDN and incentives current Pirate Services to remain with the CDN, meaning more profit for Defendant. Accordingly, Defendant’s motion to dismiss Plaintiff’s claim for vicarious infringement is denied.

#### IV. CONCLUSION

Defendant’s motion to dismiss (Dkt. 66) is denied.

SO ORDERED in No. 22-cv-00993.

Date: July 14, 2023

  
\_\_\_\_\_  
JOHN F. KNESS  
United States District Judge