

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

DISH NETWORK L.L.C.,)
Plaintiff,) Case No.
v.)
DATAACAMP LIMITED d/b/a CDN77)
and Datapacket,)
Defendant.)

COMPLAINT

Plaintiff DISH Network L.L.C. (“DISH”) sues Defendant Datacamp Limited d/b/a CDN77 and Datapacket (“Datacamp”), and states as follows:

Nature of the Action

1. DISH is the fourth largest pay-tv provider in the United States providing copyrighted programming to millions of subscribers nationwide. DISH is also one of the largest providers of international television channels in the United States offering more than 400 channels in 27 languages. Many of the international channels DISH provides are exclusive with DISH.

2. While consumers can select from a variety of legal television services, such as those offered by DISH, illegal streaming services also exist. Illegal streaming services are able to offer consumers thousands of television channels at a fraction of the cost of legal providers such as DISH because they do not pay any fees to license the content they deliver.

3. Unauthorized streaming services often depend on third-party content delivery networks, or CDNs, to deliver content to their customers. In many cases the CDN services are fundamental and necessary for a streaming service to operate.

4. Datacamp is a popular provider of CDN services to unauthorized streaming services. Datacamp materially assists these services to deliver infringing content, which includes television

channels exclusively licensed to DISH (“Protected Channels”) and the copyrighted, registered and unregistered works airing on these channels (“Works”). Datacamp offers end-to-end streaming assistance to the unauthorized services, including assisting them with transcoding and delivering the Works in HD over the internet; concealing the identities and IP addresses of the operators of the unauthorized services; and improving the speed, reliability, and overall quality of the unauthorized services (“Datacamp CDN”). On hundreds of occasions, DISH requested Datacamp to remove or disable access to the Works on the Datacamp CDN, but Datacamp failed to stop the infringement.

5. For these reasons, unauthorized streaming services are increasingly motivated to become Datacamp customers and to continue to purchase bandwidth from Datacamp. As the Motion Picture Association of America observed in a 2018 letter to the United States Trade Representative, “A growing number of globally popular illegal IPTV services use DataCamp infrastructure and services to deliver/distribute their illegal IPTV content to a worldwide audience.”¹

6. Unauthorized streaming services that Datacamp materially assists or assisted to infringe DISH’s copyrights include Banjo TV; Bollywood IPTV; Comstar TV; Express IPTV; Gennie TV; Gold TV; IPGuys; Istar; Red IPTV; Sky IPTV; and Zumm TV (together, the “Pirate Services”). The Pirate Services directly infringe or infringed DISH’s copyrights by transmitting – without authorization – the Works over the internet to users of the Pirate Services in the United States (“Service Users”). Datacamp knows that its CDN is being used by the Pirate Services to transmit the Works to users in the United States because DISH and the channel owners or their agents sent Datacamp hundreds of notices under the Digital Millennium Copyright Act (“DMCA”)

¹ See <https://www.motionpictures.org/wp-content/uploads/2018/11/notorious-markets-final.pdf>.

requesting that Datacamp remove the infringing content (“Infringement Notices”). Datacamp is ineligible for safe harbor under the DMCA for reasons including failure to terminate repeat infringers using its CDN and failure to designate an agent with the United States Copyright Office.

7. Datacamp’s infringement in connection with the Pirate Services is ongoing despite receipt of the Infringement Notices and lawsuits filed and judgments obtained against several of the Pirate Services. A court order from at least one of these cases specifically required Datacamp to disable all Datacamp IP addresses used by that respective Pirate Service to transmit the Protected Channels. But when DISH served the order on Datacamp with a letter identifying Datacamp IP addresses used by that service to transmit the Protected Channels, on multiple occasions Datacamp failed to promptly disable the reported IP addresses. DISH therefore sues Datacamp for contributory and vicarious copyright infringement.

Parties

8. Plaintiff DISH Network L.L.C. is a limited liability company organized under Colorado law, with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112.

9. Defendant Datacamp Limited is a company organized under United Kingdom law, with its principal place of business located at 207 Regent Street, London W1B 3HH. Datacamp does business as CDN77 and Datapacket, operating various websites from which it advertises and offers services under these tradenames including Datacamp.co.uk, CDN77.com, and Datapacket.com. These websites all identify Datacamp Limited as responsible for the services offered.

Jurisdiction and Venue

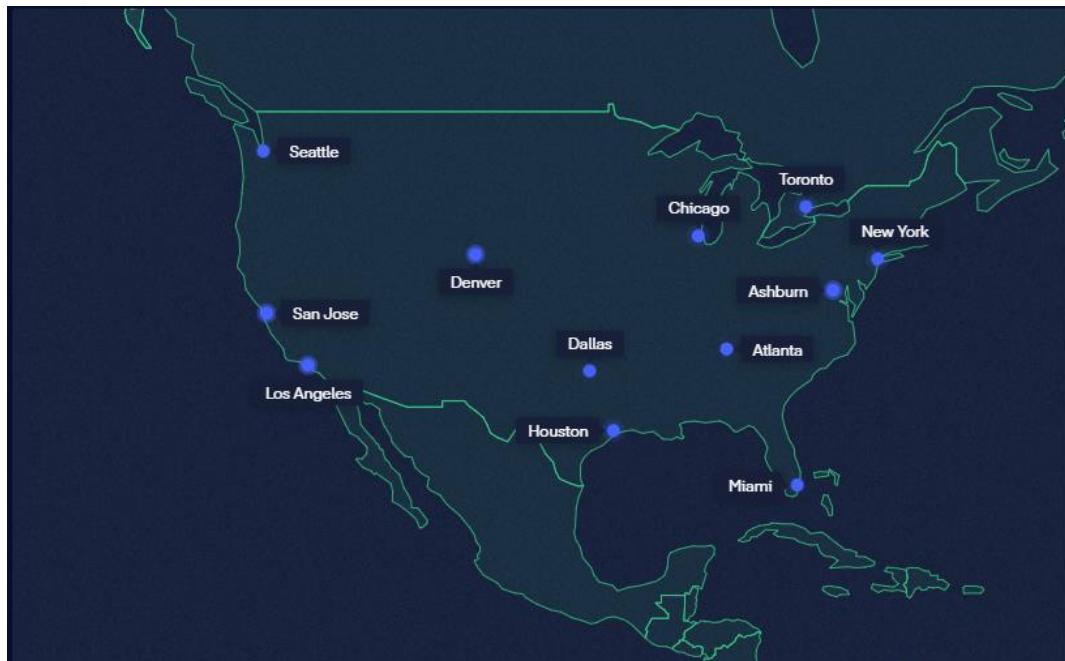
10. DISH asserts claims under the Copyright Act, 17 U.S.C. § 101 *et seq.* This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1338, and 1400.

11. This Court has personal jurisdiction over Datacamp under Fed. R. Civ. P. 4(k)(1)(a) because Datacamp purposefully directs its conduct towards and purposefully avails itself of the privileges of conducting business activities within the state of Illinois. Datacamp operates datacenters and servers in this state with which it substantially assists the Pirate Services to deliver infringing transmissions of the Works from the Protected Channels to Service Users, some of whom on information and belief reside in this state, thereby harming DISH in this state. Datacamp also operates fully interactive, commercial websites, and makes them available within this state. On information and belief, Datacamp has sold and continues to sell its services to consumers in this state.

12. Alternatively, this Court has personal jurisdiction over Datacamp under Fed. R. Civ. P. 4(k)(2). Datacamp purposely directs its activity into the United States and targets and attracts many customers and substantial revenue in the United States. This Court's exercise of jurisdiction over Datacamp is consistent with the Constitution and laws of the United States, DISH's claims arise under federal law, and Datacamp is not subject to the jurisdiction of the courts of general jurisdiction of any state.

13. Datacamp uses many United States-based sources for operating its services. Datacamp operates datacenters throughout the United States under tradenames such as CDN77 and Datapacket including in Chicago, Illinois; Ashburn, Virginia; Atlanta, Georgia; Dallas, Texas; Denver, Colorado; Houston, Texas; Los Angeles, California; Miami, Florida; New York, New

York; San Jose, California; and Seattle, Washington. Datacamp prominently touts the availability of servers in the United States on its CDN77.com and Datapacket.com websites.



Screenshot from Datapacket.com Showing Datacenter Locations in the United States²

14. Datacamp lists United States phone numbers for Sales and Support on its Datapacket.com and CDN77.com websites.

15. North America is Datacamp's second-largest source of revenue. Datacamp's North American revenue in 2020 was approximately £10.6 million, or approximately \$14.3 million.

16. Datacamp uses United States companies such as Google, Facebook, Twitter, and LinkedIn to promote its services to United States consumers.

17. Venue is proper in this Court under 28 U.S.C. § 1391(b)(2) because a substantial part of the events causing DISH's claims occurred in this district; under § 1391(b)(3) because Datacamp is subject to personal jurisdiction in this district; and under § 1391(c)(3) because as a nonresident of the United States, Datacamp may be sued in any judicial district. Venue is also

² <https://www.datapacket.com/datacenters?continent=north-america> (last visited Feb. 15, 2022).

proper in this Court under 28 U.S.C. § 1400(a) because the case involves violations of the Copyright Act.

DISH's Copyrights

18. DISH contracts for and licenses rights for the international channels transmitted on its platform from channel owners and their agents, including ARY Digital USA LLC; B4U U.S., Inc.; Bennett, Coleman and Company Limited; Hum Network Limited; MBC FZ LLC; International Media Distribution (Luxembourg) S.A.R.L.; MSM Asia Limited; National Communications Services (SMC-PVT.) Limited; Soundview ATN LLC; Soundview Broadcasting LLC; Television Media Network (Pvt) Ltd; TV Today Network Ltd.; Vedic Broadcasting Inc.; and World Span Media Consulting, Inc. DISH previously contracted for and licensed rights from Al Jazeera Media Network. Al Jazeera Media Network along with the foregoing companies are referred to as “Networks.”

19. The Networks’ channels include Aaj Tak; Aastha; Al Arabiya; Al Hayah 1; Al Jazeera Arabic News; ART Cima; ARY Digital; ATN Bangla; ATN News; B4U Movies; B4U Music; CBC; CBC Drama; Dunya TV; Express Entertainment; Express News; Future TV; Hekayat; Hum Masala; Hum Sitaray; Hum TV; Hum World; India Today; LBC; LBCI (a/k/a LDC); MBC1; MBC Drama; MBC Kids (a/k/a MBC3); MBC Masr; Melody Aflam; Melody Classic; Melody Drama; NTV Bangla; Rotana America; SAB; SET (a/k/a Sony SET); SET MAX; Times Now; and Zoom. The term “Protected Channels” used in this Complaint consists of these channels. The Networks acquire copyrights in the Works that air on their respective channels, including by producing the Works and by assignment.

20. DISH entered into signed, written licensing agreements with the Networks granting DISH the exclusive right to distribute and publicly perform the Protected Channels and Works that

air on the Protected Channels in the United States by means including satellite, over-the-top (OTT), internet protocol television (IPTV), and internet. Many of the Works that aired on the Protected Channels and for which DISH holds or held exclusive distribution and public performance rights are registered with the United States Copyright Office. (*See Exhibit 1.*) A vast number of additional, unregistered copyrighted works in which DISH holds or held exclusive distribution and public performance rights also aired on the Protected Channels. (*See Exhibit 2.*) DISH's exclusive rights in the Works were in effect when they were transmitted by the Pirate Services through the Datacamp CDN.

The Pirate Services' Massive Copyright Infringement

21. Illegal streaming services 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. These services, which include the Pirate Services, are not authorized by DISH to transmit, distribute, or publicly perform the Works in the United States, and DISH has received no compensation from them to do so.

22. The Pirate Services are advertised, marketed, and sold mainly over the internet and through retail stores. The scale of Pirate Services' infringement of the Works is massive. In general, the Pirate Services transmit the Protected Channels 24 hours per day and 7 days per week, meaning that over the last few years alone the Pirate Services have infringed over a million hours of DISH's copyrighted television programming.

23. On information and belief, most of the Pirate Services are operated by infringers located outside the United States. The Pirate Services ignored the infringement notices sent to them over the last several years.

24. Lawsuits filed by DISH and court orders obtained against certain Pirate Services likewise failed to stop the infringement.³ At least one of these court orders required Datacamp to disable all Datacamp IP addresses used to transmit the Protected Channels on the Red IPTV service. But when DISH served the court order on Datacamp with a list of Datacamp IP addresses that were being used to transmit the Protected Channels on Red IPTV, Datacamp on multiple occasions failed to promptly disable the reported IP addresses. Residing outside the United States or with no legitimate business in the United States other than illegal streaming, the Pirate Services have little incentive to comply with infringement notices or United States court orders.

Datacamp's Content Delivery Network

25. The Pirate Services rely on Datacamp's CDN services to transmit content. 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. Datacamp provides "Dedicated CDN infrastructure,"⁴ meaning that server hardware is allocated solely to individual customers' needs.⁵

26. Datacamp touts its expertise in providing optimal live streaming solutions to its customers. Datacamp claims to specialize in "live streaming processing" and assisting customers with "IPTV/OTT delivery"⁶ and tells customers to "Send us your live stream over standard

³ See *DISH Network L.L.C. v. Mo' Ayad Al Zayed Trading Est.*, No. 4:17-cv-03909, Dkt. 29 (S.D. Tex. Mar. 13, 2019) (Red IPTV); *DISH Network L.L.C. v. Atlas Elecs. Inc.*, No. 2:21-cv-12219, Dkt. 1 (E.D. Mich. Sept. 21, 2021) (Istar); *DISH Network L.L.C. v. UVCONN, Inc.*, No. 1:20-cv-01904, Dk. 22 (W.D.N.Y. Dec. 2, 2021) (Zumm TV); *DISH Network L.L.C. v. Kaczmarek*, No. 1:19-cv-04803-EK-SJB, Dkts. 42–43 (E.D.N.Y. Sept. 30, 2021) (IPGuys); *Bell Media Inc. v DOES d/b/a GoldTV*, No. T-1169-19 [2019] F.C. 1432 (Can. Ont.) (GoldTV).

⁴ See <https://www.cdn77.com/> (last visited Feb. 15, 2022).

⁵ See <https://www.webopedia.com/definitions/dedicated-server/> (updated Feb. 8, 2022).

⁶ See <https://www.cdn77.com/video-cdn> (last visited Feb. 15, 2022).

protocols...and let us convert and transcode your video...to optimize viewer experience.”⁷ As for customers’ IPTV/OTT needs, Datacamp says it “absolutely!” can help: “With CDN77 you can bring your entire video processing workflow under one roof. In fact, we’ve already helped many traditional TV broadcasters in setting up their end-to-end live streaming & VOD solutions....”⁸

27. The Datacamp CDN brings content to the end user. The Datacamp CDN also contains caching servers to accelerate load times and reduce bandwidth consumption. Each of Datacamp’s caching servers typically holds multiple storage drives with high amounts of computer memory or RAM to cache its customers’ content and seamlessly deliver it to their service users. Datacamp’s CDN caches live stream transmissions to improve latency and performance.⁹

28. Datacamp in a July 2019 blog post on CDN77.com identifies what it sees as the five main benefits of deploying a CDN for streaming services – latency; scalability and redundancy; smooth performance; security; and savings.¹⁰

29. As for latency, Datacamp says, “Among all the advantages of CDN, cutting down the network latency is the best known performance benefit. The fundament of CDN lies in strategic positioning of the servers (PoPs) closer to the end users and thus reducing the propagation time of all the data packets. Put in a simple way, when the first viewer starts watching a stream, a CDN pulls the segmented stream data from the origin server and caches it in our PoPs. Once cached, the media files remain available for other viewers. This means that all other viewers are served the video files from the closest PoP rather than from the origin, which translates into a faster and consequently smoother video distribution.”¹¹

⁷ *Id.*

⁸ *Id.*

⁹ See <https://client.cdn77.com/support/knowledgebase/live-streaming> (last visited Feb. 15, 2022).

¹⁰ See <https://www.cdn77.com/blog/live-streaming-cdn-benefits> (published July 21, 2019).

¹¹ *Id.*

30. As for scalability and redundancy, Datacamp says, “Buffering blunders often come as maddening for viewers and can easily make them go elsewhere. That’s why scalability and redundancy during the high-load conditions are two business-critical considerations for all the projects in the streaming industry operating with a global audience. By distributing the content across a high number of servers for video delivery, the result is not only a larger network backbone capacity, but very importantly, a significant offload of the origin server. Chunks packed within manifests are served to the end users in a substantial portion from the PoP’s cache instead of pulling them directly from the origin for each unique stream at once. Furthermore, by setting up a cache bypass on your stream, we make sure to cache the manifests for a second only. This converts into even more effective origin offload while providing the most up-to-date manifest available.”¹²

31. As to performance, Datacamp says, “The video in live streaming doesn’t travel through the same set of tubes to every viewer at once. Every single viewer watching streaming video has a uniquely dedicated single stream that flies through one of the countless networks and needs to be delivered consistently to avoid poor video quality. All the variables involved cause that buffering still persists and thus remains a troubling reality for many content providers. By adding a CDN segment into the streaming sequence, CDN allows for an additional playback buffer of the video chunks (i.e. chunks that ‘queue’ in the buffer until the previous chunks are played). Armed with the buffer at altogether 3 locations, namely on the side of the streaming server, CDN and the player, we maintain an uncompromised quality and uninterrupted video experience of the viewers.”¹³

¹² *Id.*

¹³ *Id.*

32. As to security, Datacamp says, “An indispensable advantage of streaming through CDN is that it comes along with all the extra security measures available on the CDN layer. When it comes to protecting the video content from unwanted attention, there are several access management and content protection features that [Datacamp] offers for free, e.g. Secure Tokens, built-in DRM, origin protection, hotlink protection or IP & geo whitelisting/blacklisting.”¹⁴

33. As to cost, Datacamp promises, “Last but not least, using CDN service brings major cost savings. Keeping your own infrastructure to handle potential peaks is expensive and often beyond the scope of the business. Letting a CDN provider handle your video assets not only comes at significantly lower expenses and more predictable costs, but it also streamlines the entire broadcasting process. Building upon own CDN infrastructure, [Datacamp] provides you with a full control of your CDN performance and gives you a detailed analytics overview thanks to a single Dashboard that integrates both CDN and Live Streaming management. This way you have a clear picture of what’s happening at each stage of the streaming pipeline.”¹⁵ By using Datacamp’s CDN the Pirate Services do not have to pay for foreign hosting services close to their customers.¹⁶

34. Datacamp assists its customers in setting up their streams and provides technical support 24 hours per day and 7 days per week to ensure that any streaming problems are quickly addressed. According to Datacamp, “live streaming always begins on your side, be it a camera or encoder. You can configure your encoder...and directly connect it to our CDN network. If that’s not an option, send us your live stream...and we will convert it and transcode your video to multi-

¹⁴*Id.*; see <https://client.cdn77.com/support/knowledgebase/security-measure/hotlink-protection> (“Our tech team can also block access from specific IPs, IP subnets or specific countries (based on the gelocation from IP) to your content.”) (Last visited Feb. 15, 2022).

¹⁵ See <https://www.cdn77.com/blog/live-streaming-cdn-benefits> (published July 21, 2019).

¹⁶ See <https://client.cdn77.com/support/knowledgebase/introduction-cdn/benefits-cdn> (last visited Feb. 15, 2022).

bitrate profiles [to] optimise the viewing experience.”¹⁷ Datacamp further notes that live-streaming typically requires a “custom solution” and therefore customers should contact Datacamp to find the streaming solution right for them.¹⁸

Datacamp Substantially Assists the Pirate Services to Transmit the Works.

35. Datacamp transmits the Works aired on the Protected Channels on the Pirate Services to Service Users – an act that by itself is a material contribution to the Pirate Services’ direct infringement. Datacamp also provides additional services that substantially assist the Pirate Services’ infringement.

A. Datacamp Provides End-to-End Live Streaming Assistance to the Pirate Services.

36. Datacamp offers end-to-end assistance to the Pirate Services, from encoding Protected Channel feeds into signals capable of being transmitted efficiently over a CDN to securing the transmissions to make them accessible only to individuals permitted by the Pirate Services.

37. The Pirate Services take legitimate content from cable/satellite/terrestrial TV and make it available through the internet so a Service User with a set-top box, smart TV, PC, or mobile device can view it. Converting TV content from its original format to an internet signal delivered to the Service User through a CDN is complex – for instance, because the Pirate Services desire to provide maximum video quality to Service Users using various devices and internet connection speeds. Service Users may switch to a competitor’s service if video quality is lacking. Without Datacamp’s CDN services and expertise, the Pirate Services could not do what they are doing.¹⁹

¹⁷ See <https://client.cdn77.com/support/knowledgebase/live-streaming> (last visited Feb. 15, 2022).

¹⁸ *Id.*

¹⁹ See <https://www.cdn77.com/blog/live-streaming-cdn-benefits> (published July 21, 2019) (“Be it live, linear or OTT broadcast, a single streaming server often does not satisfy the performance needs especially when it comes to reaching a global audience.”).

38. On information and belief, Datacamp addresses this complexity, in part, by assisting the Pirate Services to convert the Protected Channel feeds into “multi-bitrate profiles” that automatically change the quality of the stream for each viewer depending on their device and internet connection speed.²⁰ The Pirate Services can more easily convince Service Users that their services are legitimate and worth paying for by providing HD-quality streams with limited buffering.

39. Datacamp also offers to guard transmissions of the Works from those that might try to steal or access it without authorization of the Pirate Services. The Pirate Services must be able to encrypt their streams so that only subscription-paying customers can view them. Unencrypted streams are freely accessible and therefore cannot be monetized like encrypted streams. Datacamp offers the Pirate Services security solutions such as “Secure Token” and “built-in DRM” to shield the Works from “unwanted attention.”²¹

40. Without media security services provided by Datacamp, the Pirate Services would be unable to control access to their streams and therefore be less able to charge customers a premium.

B. Datacamp Significantly Improves the Quality of the Pirate Services, Helping Them Deliver the Works to a Wider Audience.

41. Datacamp improves the performance of the Pirate Services by reducing the physical distance between the Service User and the channel streams and improving the server-side infrastructure, such as through load balancing and caching. These optimizations materially increase the quality of the Pirate Service’s streaming product.

²⁰ See <https://client.cdn77.com/support/knowledgebase/live-streaming> (last visited Feb. 15, 2022).

²¹ See <https://client.cdn77.com/support/knowledgebase/security-measure> (last visited Feb. 15, 2022).

42. Datacamp decreases the Pirate Services’ server load through “[t]he strategic placement of [Datacamp’s] PoPs,” thereby increasing the “[n]umber of concurrent users [the Pirate Services] can serve....”²²

43. With Datacamp’s CDN, the Pirate Services’ “[r]esponse time & reliability will get a boost” because “High-performing...applications equal a high conversion rate [and] [l]atency and speed-related issues tend to harm web businesses and lead to an unpleasant user experience.”²³ According to Datacamp, “Just a few seconds [of delay] can mean the difference between a successful conversion or a bounce.”²⁴ Datacamp increases the Pirate Services’ load speeds, giving their “online brand[s] a[] boost....”²⁵ In short, Datacamp allows the Pirate Services to deliver a more attractive, competitive product, which equates to more Service Users and a wider audience to view infringing transmissions of the Works.

44. Datacamp also offers the Pirate Services add-ons such as DVR and time-shifting.²⁶ These features are especially important in delivering non-United States television channels such as the Protected Channels because these channels’ programming schedules, which are based on distant time zones, are often inconvenient for a United States audience. With DVR and time-shifting the Pirate Services can attract more Service Users by providing their Service Users with a way to watch the Works at a time other than when the Works first air. Pirate Services can also use DVR and time-shifting functionality to attract more Service Users by convincing them that the Pirate Services are

²² See <https://client.cdn77.com/support/knowledgebase/introduction-cdn/benefits-cdn> (last visited Feb. 15, 2022).

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ See <https://client.cdn77.com/support/knowledgebase/live-streaming/live-to-vod> (last visited Feb. 15, 2022).

offering licensed services because DVR and time-shifting are popular features offered by authorized, legitimate providers such as DISH.

C. Datacamp Conceals the Identities of the Pirate Service Operators.

45. The Works on the Protected Channels are routed through Datacamp's CDN instead of the origin servers maintained by the Pirate Services. This process conceals the origin servers maintained by the operators of the Pirate Services. Concealing this information prevents DISH from sending infringement notices directly to the internet service providers for the origin servers.

46. To avoid liability for replacing content (or restoring access to content) that is the subject of a takedown request, the DMCA requires service providers like Datacamp to have their customers provide a DMCA-compliant counter notice. *See* 17 U.S.C. § 512(g)(3). A DMCA-compliant counter notice must include the name, address, and phone number of the service provider's customer. *Id.*

47. Datacamp did not remove or disable access to the content identified in the Infringement Notices – nor did it require its customers to submit DMCA-compliant counter notices, which would have identified the operators of the Pirate Services to DISH.

D. Datacamp Makes Temporary Copies of, or Caches, the Works.

48. Service Users log into the Pirate Services from internet-enabled devices such as a set-top box, smart TV, PC, or mobile device, and then select the Protected Channels from the Pirate Services' electronic channel guides.

49. The Protected Channels are then transmitted to the Service Users through the Datacamp CDN and the Works currently airing on the selected channel proceed to play on the Service Users' devices.

50. The Works are delivered to the Service Users from servers within Datacamp's network in geographic proximity with the viewer. These servers make temporary copies of, or cache, the Works as the Service Users access them from the Pirate Services.

51. A temporary copy of the Works is also caused to be made in the computer memory of the Service Users' devices.

Datacamp's Lax Infringement Policy

52. Since at least October 2017, Datacamp has deliberately refused to take reasonable measures to stop the Pirate Services from using its CDN to infringe DISH's copyrights – even after Datacamp learned of their specific and repeated acts of infringement including the names of the Pirate Services, their IP addresses, domain names, and the URLs used to transmit the Works.

53. Infringement Notices were sent to Datacamp advising it of the Pirate Services' blatant and systematic use of the Datacamp CDN to transmit, distribute, and publicly perform the Works to Service Users:

- 68 notices were sent to Datacamp about Istar since October 9, 2017.
- 80 notices were sent to Datacamp about Red IPTV since May 15, 2018.
- 67 notices were sent to Datacamp about Zumm TV since August 28, 2018.
- 40 notices were sent to Datacamp about Gold TV since March 1, 2019.
- 22 notices were sent to Datacamp about IPGuys since April 5, 2019.
- 44 notices were sent to Datacamp about Express IPTV since April 15, 2019.
- 16 notices were sent to Datacamp about Bollywood IPTV since August 27, 2020.
- 12 notices were sent to Datacamp about Gennie TV since September 28, 2020.
- 21 notices were sent to Datacamp about Banjo TV since November 12, 2020.
- 10 notices were sent to Datacamp about Comstar TV since January 10, 2021.
- 21 notices were sent to Datacamp about Sky IPTV since June 11, 2021.

54. Datacamp customers responsible for providing the Works on various Pirate Services did so repeatedly, and continued to do so even after DISH complained to Datacamp. These

Datacamp customers used the same IP addresses, domain names, and URLs to deliver infringing content for the same Pirate Services. (See Exhibits 3–13.)

55. Upon receiving Infringement Notices, Datacamp 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.

56. DISH and the Networks in response to Datacamp’s requests provided more information about the Pirate Services, including evidence of infringement taking place on Datacamp’s servers in the form of screenshots of transmissions of the Works and network traffic recorded in the form of PCAP files, showing that Datacamp’s servers were responsible for the infringing transmissions on the Pirate Services.



Example of Screenshot and PCAP Evidence Sent to Datacamp about the Istar Pirate Service’s Use of Datacamp’s CDN to Illegally Transmit the MBC Kids (MBC3) Channel

57. Datacamp failed to remove or block the Protected Channels or the Works from being transmitted through its servers and failed to terminate the Pirate Services responsible for the infringement, despite receiving the Infringement Notices and other evidence provided by DISH and Networks. Datacamp’s CEO Zdenek Cendra 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 DISH and Networks reported. But Datacamp did not get more strict with its customers, did not remove or disable access to the infringing content, and apparently did not terminate its customers’ accounts, even after acknowledging numerous copyright violations.

58. In addition to requiring customers to submit DMCA-compliant counter notices in response to Infringement Notices, there are several other actions Datacamp could have taken, but failed to take, to remove or disable access to particular content/URLs that DISH reported.

59. Datacamp could have found out whether the Pirate Services were legally authorized to transmit the Works by first requiring them to verify their rights before transcoding the Works or transmitting them to Service Users.

60. Datacamp could have responded, or responded more promptly, to the Infringement Notices.

61. Datacamp, on receipt of the Infringement Notices, could have investigated to determine whether infringement was occurring rather than accepting false and unsupported assertions from the Pirate Services that there was no infringement or that prior infringement had ceased.

62. Datacamp could have implemented a multi-strike policy, such as by temporarily suspending a Pirate Service's CDN account on receipt of one infringement notice against that account and then permanently terminating the account on receipt of additional notices. By failing to implement any of these reasonable measures to combat copyright infringement, Datacamp provided an open invitation for customers to use the Datacamp CDN as a tool of infringement.

Datacamp's Control Over and Direct Financial Benefit in the Pirate Services

63. Datacamp has the right and ability to stop or limit the Pirate Services' infringement by geoblocking in the United States the transmissions of the Works on the Protected Channels and by terminating the Pirate Services' access to the Datacamp CDN altogether. The Pirate Services cannot offer a viable streaming service without a CDN, and Service Users would likely have to look

elsewhere, for example to DISH – a legitimate source of the Works, if the Pirate Services were not able to transmit content through a CDN.

64. Datacamp’s service agreements with customers permit it to remove or block access to the Works or terminate the Pirate Services’ accounts for “any reason.”²⁷ Rather than exercise that right and ability to shut off its services to infringers, Datacamp turned a blind eye, making the Datacamp CDN a safe haven for the Pirate Services’ infringement.

65. Datacamp receives a direct financial benefit from the Pirate Services. The Pirate Services are motivated to sign up with, remain with, and pay Datacamp for bandwidth to transmit the Works on the Protected Channels because of Datacamp’s lax policy towards infringement.

66. The Pirate Services cater to consumers of international television content. The Protected Channels consist of some the most popular international channels. The Pirate Services are therefore drawn to the Datacamp CDN because of Datacamp’s lax attitude towards transmission of the Protected Channels in particular.

67. Datacamp has actual knowledge of the Pirate Services’ infringement because of the Infringement Notices and other evidence DISH and Networks provided. But rather than put a stop to the Pirate Services’ infringement, Datacamp prioritized its own profits over its legal obligations.

68. Datacamp’s interests are aligned with the Pirate Services. Datacamp’s profits increased as the Pirate Services attracted new, paying Service Users. This is so because CDNs like Datacamp charge customers more as their bandwidth consumption increases. The amount of bandwidth the Pirate Services use is, at least to some extent, a function of the number of Service Users they have. If Datacamp removed the Protected Channels from the Datacamp CDN, the Pirate Services’ bandwidth usage would decrease. If Datacamp geoblocked the Protected Channels in the

²⁷ See <https://www.cdn77.com/terms-and-conditions> (last visited Feb. 15, 2022).

United States, this also would reduce bandwidth, unless the Service Users replaced viewing time with other channels. But given the popularity of the Protected Channels, this is unlikely. All of these facts explain why Datacamp is so reluctant to stop the Pirate Services' infringement – as the Pirate Services attract new Service Users and retain existing ones, Datacamp's profits also increase.

69. By enabling the Pirate Services' copyright infringement, Datacamp increased its revenues. Datacamp's North American and worldwide revenues increased by over 150% from 2018 to 2020.²⁸ At least some of this increase is attributable to the revenues Datacamp earned from the Pirate Services, which it would not have earned had Datacamp adequately policed infringement on its CDN.

Datacamp Has No Right to Any DMCA Safe Harbor

70. Congress created a safe harbor in the DMCA that limits the liability of service providers for copyright infringement under certain situations. *See* 17 U.S.C. § 512. This limitation of liability under the safe harbor applies “[o]nly if the service provider...has adopted and reasonably implemented, and informs subscribers and account holders of...a policy that provides for the termination in appropriate circumstances of subscribers and account holders...who are repeat infringers. *Id.* § 512(i)(1)(A).

71. When the service provider stores copyrighted material on their network at the direction of the user, as Datacamp does, the service provider must also satisfy additional conditions to benefit from the safe harbor, including (i) “act[ing] expeditiously to remove, or disable access to, the material” when the service provider obtains “knowledge or awareness” the material is infringing, (ii) “not receiv[ing] a financial benefit directly attributable to the infringing activity...”

²⁸ According to its annual reports, Datacamp's North American revenues increased from £3.9 million in 2018 to £10.6 million in 2020 and worldwide revenues increased from £13.9 million to £36.2 million.

[when] the service provider has the right and ability to control such activity,” (iii) “designat[ing] an agent to receive notifications of claimed infringement...by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office...the name, address, phone number, and electronic mail address of the agent,” and (iv) “upon notification of a claimed infringement...respond[ing] expeditiously to remove, or disable access to, the material that is claimed to be infringing.” *Id.* § 512(c).

72. Datacamp has no right to any safe harbor under the DMCA because it has not satisfied the necessary conditions.

73. Datacamp failed to designate a DMCA agent to receive notifications of claimed infringement or provide the agent’s contact information on Datacamp’s websites or with the United States Copyright Office.

74. Datacamp has not acted expeditiously to remove or disable access to infringing material on its servers or implemented a repeat-infringer policy. Some of the same Datacamp servers were used repeatedly by the Pirate Services for infringement dating back to October 2017, despite at least 401 Infringement Notices identifying the IP addresses, domain names, and URLs being used to transmit the Works. (*See* Exhibits 3-13.) The data show that Datacamp has not adopted and reasonably implemented a policy to reduce infringement by terminating subscribers or account holders who are repeat infringers.

75. Datacamp has derived an obvious and direct financial benefit from the Pirate Services’ infringement. The Datacamp CDN was used to publicly perform thousands of Works to an unknown number of Service Users, serving as a draw for Datacamp to attract and retain the Pirate Services, and charge them additional fees. By failing to terminate the accounts of the Pirate Services, Datacamp obtained a direct financial benefit from the Pirate Services’ infringing activity

in the form of illicit revenue that it would not have received had it terminated the Pirate Services' accounts. Indeed, because Datacamp charges based on bandwidth used by its customers, Datacamp had an interest in the Pirate Services transmitting as much as possible through the Datacamp CDN. On information and belief, Datacamp decided not to terminate the Pirate Services' accounts or remove or disable access to the Works because it wanted to maintain the revenue that would come from the accounts.

CLAIMS FOR RELIEF
Count I

Materially Contributing to Copyright Infringement under 17 U.S.C. § 501

76. DISH repeats and realleges the allegations in paragraphs 1-75.

77. DISH is a copyright owner under 17 U.S.C. § 106 because DISH holds or held exclusive rights to publicly perform the Works in the United States by means including satellite, OTT, IPTV, and internet.

78. The Works are original audiovisual works fixed in a tangible medium of expression, and are therefore copyrightable subject matter. DISH's copyrights in the Works arise under laws of nations other than the United States that are parties to copyright treaties with the United States, including the United Arab Emirates, Qatar, Egypt, Lebanon, Pakistan, India, and Bangladesh, where the programs were authored and first published. Under 17 U.S.C. §§ 101 and 411, the Works are non-United States works and therefore registration with the United States Copyright Office is not a prerequisite to filing a copyright infringement action for the Works.

79. DISH's exclusive rights to publicly perform the Works, including those identified in Exhibits 1-2, are directly infringed by the Pirate Services' unauthorized transmission of these works to Service Users who access the works. The Pirate Services use the Datacamp CDN to publicly perform the Works.

80. Datacamp materially contributes to the Pirate Services' direct infringement of DISH's exclusive public performance rights. Through the Infringement Notices, Datacamp had actual knowledge that the transmission of the Works to Service Users infringes DISH's exclusive public performance rights and that the Datacamp CDN was being used for such copyright infringement on a massive scale. Datacamp also had actual knowledge that its subscribers, the Pirate Services, engaged in repeated and willful copyright infringement. Datacamp facilitated, encouraged, and materially contributed to the Pirate Services' infringement by continuing to provide its services, servers, and the facilities necessary for the Pirate Services to commit repeated infringement.

81. Datacamp had the means to withhold its assistance to the Pirate Services upon learning of the URLs, domain names, and IP addresses associated with the servers providing access to the Works, including by removing or disabling access to the Works or terminating the Pirate Services' accounts, but Datacamp failed to do so. Datacamp could have taken these simple measures to prevent further infringement of DISH's exclusive rights to publicly perform the Works.

82. By purposely ignoring or turning a blind eye to the Pirate Services' willful and repeated infringement, Datacamp knowingly caused and materially contributed to the unauthorized public performance of the Works, in violation of DISH's exclusive rights.

83. Datacamp's actions are willful, malicious, intentional, purposeful, and in disregard of and with indifference to the rights of DISH.

84. Unless enjoined by the Court, Datacamp will continue to engage in acts causing substantial and irreparable injury to DISH that includes damage to its reputation, loss of goodwill, and lost sales, for which there is no adequate remedy at law.

Count II

Vicarious Copyright Infringement under 17 U.S.C. § 501

85. DISH repeats and realleges the allegations in paragraphs 1-75 and 77-79.

86. Datacamp is liable as a vicarious copyright infringer for the Pirate Services' direct infringement of DISH's exclusive public performance rights.

87. Datacamp has the legal right and the actual ability to supervise and control the infringing activities of the Pirate Services through the Datacamp CDN. Datacamp failed to stop the infringement of DISH's exclusive rights in the Works.

88. The Pirate Services are motivated to become Datacamp subscribers due to their knowledge that they can publicly perform the Works without interference from Datacamp because Datacamp continually failed to take meaningful action to reduce infringement in response to the Infringement Notices.

89. At all relevant times, Datacamp had a financial interest in, and derived direct financial benefit from, the Pirate Services' infringing use of the Datacamp CDN. The Datacamp CDN was used to publicly perform thousands of Works to an unknown number of Service Users, serving as a draw for Datacamp to attract, retain, and charge more fees to its customers. By failing to terminate the Pirate Services' accounts and remove or disable access to the Works, Datacamp profited from illicit revenue that it would not otherwise have received.

90. Datacamp's actions are willful, malicious, intentional, purposeful, and in disregard of and with indifference to the rights of DISH.

91. Unless enjoined by the Court, Datacamp will continue to engage in acts causing substantial and irreparable injury to DISH that includes damage to its reputation, loss of goodwill, and lost sales, for which there is no adequate remedy at law.

PRAYER FOR RELIEF

DISH prays for judgment against Datacamp as follows:

A. For a permanent injunction under 17 U.S.C. § 502 against Datacamp, and any of its officers, agents, servants, employees, attorneys, or other persons acting in active concert or participation with any of the foregoing that receives actual notice of the order, the terms of which include:

1. enjoining or restraining any act of inducing or contributing to another's conduct of transmitting, streaming, distributing, or publicly performing in the United States, with the Pirate Services or any other device, application, service, or process, any of the Aastha; Al Hayah 1; ART Cima; ATN Bangla; ATN News; B4U Movies; B4U Music; CBC; CBC Drama; Express News; Future TV; Hekayat; LBC; LBCI (a/k/a LDC); Melody Aflam; Melody Classic; Melody Drama; NTV Bangla; Rotana America; SAB; SET (a/k/a Sony SET); SET MAX; Times Now; and Zoom channels ("Injunction Channels") or any of the programming that comprises any of the Injunction Channels;

2. ordering the termination of the current and future accounts of the Pirate Services;

3. enjoining the use of any Datacamp server to provide the Injunction Channels or any of the programming that comprises any of the Injunction Channels; and

4. ordering that Datacamp adopt and implement a policy that provides for the prompt termination of subscribers that engage in repeat infringement of the Injunction Channels or any of the programming that comprises any of the Injunction Channels.

B. For 217 or more registered works, statutory damages as awarded by the Court up to \$150,000 per registered work infringed under 17 U.S.C. § 504(c), or Datacamp's profits attributable to the infringement of those registered works under 17 U.S.C. § 504(b).

C. For unregistered works, an award of Datacamp's profits attributable to the infringement of each unregistered work under 17 U.S.C. § 504(b).

D. For DISH's attorneys' fees and costs under 17 U.S.C. § 505.

E. For impoundment and disposition of all infringing articles under 17 U.S.C. § 503.

F. For pre- and post-judgment interest on all monetary relief, from the earliest date permitted by law at the maximum rate permitted by law.

G. For such additional relief as the Court deems just and equitable.

Respectfully submitted,

Dated: February 25, 2022

LEWIN VERVENIOTIS LAW GROUP

By: /s/ David M. Lewin
David M. Lewin
120 North LaSalle, Suite 2600
Chicago, IL 60602
Telephone: (312) 725-2084
DML@LewVer.com

HAGAN NOLL & BOYLE LLC

Stephen M. Ferguson (*pro hac vice* to be filed)
David M. Korn (*pro hac vice* to be filed)
Two Memorial City Plaza
820 Gessner, Suite 940
Houston, TX 77024
Telephone: (713) 343-0478
Facsimile: (713) 758-0146

Attorneys for Plaintiff DISH Network L.L.C.