

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO**

Civil Action No. 1:21-cv-1261-NYW-SKC

MILLENNIUM FUNDING, INC.,
VOLTAGE HOLDINGS, LLC,
LHF PRODUCTIONS, INC.,
OUTPOST PRODUCTIONS, INC.,
AFTER II MOVIE, LLC,
MILLENNIUM MEDIA, INC.,
WONDER ONE, LLC,
HITMAN TWO PRODUCTIONS, INC.,
MILLENNIUM IP, INC.,
I AM WRATH PRODUCTIONS, INC.,
KILLING LINK DISTRIBUTION, LLC,
VENICE PI, LLC,
RAMBO V PRODUCTIONS, INC.,
MON, LLC,
NIKOLA PRODUCTIONS, INC.,
BODYGUARD PRODUCTIONS, INC.,
YAR PRODUCTIONS, INC.,
DALLAS BUYERS CLUB, LLC,
SF FILM, LLC,
SCREEN MEDIA VENTURES, LLC,
SPEED KILLS PRODUCTIONS, INC.,
LAUNDRY FILMS, INC.,
CINELOU FILMS, LLC,
BADHOUSE STUDIOS, LLC,
HANNIBAL CLASSICS INC., and
JUSTICE EVERYWHERE PRODUCTIONS LLC,

Plaintiffs,

v.

PRIVATE INTERNET ACCESS, INC.,

Defendant.

FOURTH AMENDED COMPLAINT AND JURY DEMAND

Plaintiffs MILLENNIUM FUNDING, INC., VOLTAGE HOLDINGS, LLC, LHF PRODUCTIONS, INC., OUTPOST PRODUCTIONS, INC., AFTER II MOVIE, LLC, MILLENNIUM MEDIA, INC., WONDER ONE, LLC, HITMAN TWO PRODUCTIONS, INC., MILLENNIUM IP, INC., I AM WRATH PRODUCTIONS, INC., KILLING LINK DISTRIBUTION, LLC, VENICE PI, LLC, RAMBO V PRODUCTIONS, INC., MON, LLC, NIKOLA PRODUCTIONS, INC., BODYGUARD PRODUCTIONS, INC., YAR PRODUCTIONS, INC., DALLAS BUYERS CLUB, LLC, SF FILM, LLC, SCREEN MEDIA VENTURES, LLC, SPEED KILLS PRODUCTIONS, INC., LAUNDRY FILMS, INC., CINELOU FILMS, LLC, BADHOUSE STUDIOS, LLC, HANNIBAL CLASSICS INC., and JUSTICE EVERYWHERE PRODUCTIONS LLC (“Plaintiffs”) file this Fourth Amended Complaint against Defendant PRIVATE INTERNET ACCESS, INC., (“Defendant PIA”) and allege as follows:

I. INTRODUCTION

1. An individual that pirates copyright protected content in the United States from her home Internet service via peer-to-peer (P2P) networks such as the BitTorrent Protocol puts herself in great legal peril because her Internet Protocol (“IP”) address is publicly exposed. A copyright owner can subpoena her Internet service provider for log records to obtain her subscriber identification and seek statutory damages for copyright infringement that can be as high as \$150,000. This risk is known among prolific pirates and feared.

2. Against this background, Defendant promotes its Virtual Private Network

(“VPN”) services as an essential tool for individuals who wish to pirate content using P2P networks by emphasizing that it provides end users “anonymous” usage by, for example, deleting end users’ log access records so that their identities cannot be disclosed to copyright owners.

3. Defendant even promotes its VPN services as essential tools to use notorious piracy applications and access torrent files from notorious movie piracy websites such as YTS without getting caught.

4. As discussed below, although Defendant PIA attempts to use the codeword “privacy”, employees of Defendant PIA explicitly advocate use of its service for piracy – one is even a member of “The Pirate Party” – and participate in the operation of the notorious website The Pirate Bay. Even worse, after Defendant PIA was served with a subpoena for identification of one its end users that accessed pirated content from the website YTS using its VPN service, Defendant PIA issued a warning to its end users that Plaintiffs’ counsel was “extorting” YTS users.

5. Emboldened by Defendant’s promises that their identities cannot be disclosed, Defendant’s end users use their VPN services not only to engage in widespread movie piracy, but other outrageous criminal conduct such as harassment and illegal hacking. When these crimes become public, Defendant uses these tragic incidents as opportunities to boast about its VPN service.

II. NATURE OF THE ACTION

6. This matter arises under the United States Copyright Act of 1976, as

amended, 17 U.S.C. §§ 101, et seq. (the “Copyright Act”).

7. The Plaintiffs allege that Defendant is secondarily liable for copyright infringements and violations under the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 1202.

8. The Plaintiffs allege that Defendant PIA is liable for breach of contract in violation of the laws of Colorado and/or Hawaii.

III. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 17 U.S.C. §§ 101, et. seq., (the Copyright Act), 28 U.S.C. § 1331 (federal question), 28 U.S.C. § 1338 (patents, copyrights, trademarks, and unfair competition) and 28 U.S.C. § 1367(a) (supplemental jurisdiction).

10. Defendant solicits, transacts, and/or does business within this jurisdiction, and has committed unlawful and tortious acts both within and outside this jurisdiction with the full knowledge that its acts would cause injury in this jurisdiction. As such, Defendant has sufficient contacts with this judicial district to permit the Court’s exercise of personal jurisdiction over it.

11. Defendant leases servers and is assigned Internet Protocol (“IP”) addresses at non-party Sharktech’s data center in Denver, Colorado.

12. Defendant PIA’s corporate office is in Greenwood Village, Colorado. See <https://www.privateinternetaccess.com/about-us> [last accessed on Nov. 5, 2021] (PIA Corporate office at 5555 DTC Parkway, Suite 360, Greenwood Village, Colorado).

13. Plaintiffs’ injuries arise out of Defendant’s forum-related activities, namely

Defendant's contribution to infringements of Plaintiffs' copyright protected Works, and DMCA violations at IP addresses and servers controlled by Defendant in this District.

14. Plaintiffs' injuries arise out of Defendant's breach of a settlement agreement to resolve claims alleged in this case such as *inter alia* the First Amended Complaint.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) - (c) because: (a) all or a substantial part of the events or omissions giving rise to the claims occurred in this District; (b) the Defendant can or could be found, in this District; and/or (c) Defendant is subject to the court's personal jurisdiction with respect to the present action. Additionally, venue is proper in this District pursuant 28 U.S.C. § 1400(a) (venue for copyright cases), because the Defendant or Defendant's agents reside and can be found in this District.

IV. PARTIES

A. The Plaintiffs

16. The Plaintiffs are the owners of the copyrights in the Works shown in Exhibit "1".

17. Each of Plaintiffs LHF Productions, Inc., Millennium Funding, Inc., Outpost Productions, Inc., Millennium Media, Inc., Hitman Two Productions, Inc., Millennium IP, Inc., Rambo V Productions, Inc., Nikola Productions, Inc., and Bodyguard Productions, Inc. is a corporation organized under the laws of the State of Nevada, has a principal office in Nevada and is an affiliate of Millennium Media, Inc. a production company and distributor of a notable catalog of major motion pictures.

18. Each of Plaintiffs Voltage Holdings, LLC and After II Movie, LLC is a limited

liability company registered under the laws of the State of Nevada, has principal offices in Los Angeles, California and is an affiliate of Voltage Pictures, a production company with a notable catalog of major award-winning motion pictures.

19. MON, LLC is a limited liability company registered under the laws of the California, having principal office in Beverly Hills, California and is an affiliate of Voltage Pictures.

20. Venice PI, LLC is a limited liability company registered under the laws of the State of California, having principal office in Los Angeles, California and is an affiliate of Voltage Pictures.

21. Wonder One, LLC is a Wyoming limited liability company with its principal place of business in Sherman Oaks, CA.

22. I am Wrath Production, Inc. is a California corporation with its principal place of business in Los Angeles, CA.

23. Killing Link Distribution, LLC is a California limited liability company with its principal place of business in Beverly Hills, CA 90212.

24. YAR Productions, Inc. is a New York corporation with its principal place of business at Monsey, New York.

25. Dallas Buyers Club, LLC is a Texas limited liability company with its principal place of business at The Woodlands, TX.

26. SF Film, LLC is a New York limited liability company with its principal place of business at Albany, New York.

27. Screen Media Ventures, LLC is a Delaware limited liability company with its

principal place of business at New York, NY.

28. SPEED KILLS PRODUCTIONS, INC. is a Wyoming corporation with its principal place of business at West Hollywood, CA.

29. LAUNDRY FILMS, INC. is a California corporation with its principal place of business in Venice, California.

30. CINELOU FILMS, LLC is a California limited liability company with its principal place of business in California.

31. BADHOUSE STUDIOS, LLC is a Wyoming limited liability company with its principal place of business at West Hollywood, CA.

32. HANNIBAL CLASSICS INC., is a California corporation with its principal place of business at West Hollywood, CA.

33. JUSTICE EVERYWHERE PRODUCTIONS LLC is a Georgia limited liability company with its principal place of business at Los Angeles, CA, 90067.

B. The Defendant

34. Defendant PIA is, upon information and belief, a corporation organized under the laws of Indiana with its principal place of operation in Colorado.

35. Non-party Kape Technologies PLC (“Kape”) is, upon information and belief, a foreign company incorporated in the Isle of Man and is the owner of Defendant PIA.

36. Kape was previously known as Crossrider until it changed its name change in 2018.

37. Kape and PIA are mere alter egos.

38. PIA and Kape have many of the same corporate officers.

39. Upon information and belief, Moran Laufer is an officer of both PIA and Kape.

40. PIA and Kape share many of the same resources. Employees of PIA use email addresses with domain KAPE.COM identifying themselves as employees of Kape.

41. PIA and Kape fail to maintain corporate formalities of separate existence. Employees of PIA use email addresses with domain kape.com identifying themselves as employees of Kape.

42. Upon information and belief, Kape pays the salaries and expenses of employees of PIA.

43. Kape directs and dictates the business decisions of PIA. For example, Dr. Venetia Argyropoulou, an officer of Kape and, upon information and belief, a resident of Cyprus and a practicing lawyer in Greece and Cyprus directs and dictates legal decisions for PIA including the decision for PIA to breach a settlement agreement with Plaintiffs.

44. Dr. Argyropoulou even dictates mundane decisions of PIA such as whether the general counsel of PIA could execute a waiver of personal service in this action.

45. There is such a unity of interest between Kape and PIA that the individuality, or separateness, of Kape and PIA have ceased and the facts are such that an adherence to the fiction of the separate existence of PIA and Kape would, under the particular circumstances, sanction a fraud or promote injustice.

46. Kape is owner of the VPN services CyberGhost and ZenGuard.

47. Kape is the owner and/or exercises effective control of publications such as VPNMENTOR.COM and WIZCASE.COM.

48. As explained below, Kape promotes its VPN services PIA and CyberGhost explicitly for piracy in its publications.

49. Defendant leases servers from data centers across the world and are allocated IP addresses from said data centers.

50. Defendant leases servers from Sharktech in Denver, CO and were allocated IP addresses from Sharktech.

51. As discussed more fully below, Defendant purposefully chooses data centers that do not publish reassignments of their IP address assignments/allocations to Defendant.

52. Defendant provides VPN services to its customers (“end users”).

53. A VPN is a type of Internet Service that provides access to the Internet. A conventional ISP will assign its end user an IP address and log the end users’ access to the Internet while using the assigned IP address. In comparison, many VPN providers provide their end users “anonymous” usage by, for example, deleting end users’ log access records, assigning their end users IP addresses that are simultaneously shared among many users, and/or encrypting traffic.


54. Defendant promotes its VPN services as a tool that can be used to pirate copyright protected content without getting caught.

55. Upon information and belief, PIA engages in the same conduct as its end users. PIA proudly employs as its head of “Privacy” Rick Falkvinge, the founder of the first “Pirate Party” whose aim is to abolish intellectual property laws. <https://www.privateinternetaccess.com/blog/author/rick/> [last accessed on 11/4/2021].

privateinternetaccess.com/blog/author/rick/

Privacy News Online
by Private Internet ACCESS

PIA Homepage Privacy News Contact



Rick Falkvinge

Rick is Head of Privacy at Private Internet Access. He is also the founder of the first Pirate Party and is a political evangelist, traveling around Europe and the world to talk and write about ideas of a sensible information policy. Additionally, he has a tech entrepreneur background and loves good whisky and fast motorcycles.

[Web](#) | [Twitter](#) | [Reddit](#) | [More Posts\(350\)](#)

56. Rick Falkvinge states that a reason to use a VPN service that “create no logs” is to avoid “the people behind Expendables 3 are on a suing spree”.

It’s also interesting to see how effective VPNs are at protecting end-users who manufacture unlicensed copies of knowledge and culture from the monopolized copyright industry – apparently, the people behind Expendables 3 are on a suing spree, but hitting a no-log VPN on an end-address is literally a dead end – there’s nowhere to go from there. (Which is another reason to only use VPN services that a) create no logs, b) don’t demand personal information in the first place – like allowing payment with bitcoin.)

<https://www.privateinternetaccess.com/blog/with-the-copyright-industry-disliking-vpns-in-public-you-know-theyre-doing-good/> [last accessed on Nov. 4, 2021].

privateinternetaccess.com/blog/with-the-copyright-industry-disliking-vpns-in-public-you-know-theyre-doing-good/

copyright industry is yapping about here. (Also, it should be noted that the Hulu service is already mistreating its customers in this way.)

The next step is predictable from the SOPA debate – it’s pressuring payment providers to **refuse service** to VPN services, in a blatant display of the cartelization of the few payment providers. (There’s a double reason to only use a VPN that accepts bitcoin, right there: try shutting off bitcoin payments.)

It’s also interesting to see how effective VPNs are at protecting end-users who manufacture unlicensed copies of knowledge and culture from the monopolized copyright industry – apparently, the people behind Expendables 3 are on a **suing spree**, but hitting a no-log VPN on an end-address is literally a dead end – there’s nowhere to go from there. (Which is another reason to only use VPN services that a) create no logs, b) don’t demand personal information in the first place – like allowing payment **with bitcoin**.)

57. Some of the Plaintiffs in this action such as Millennium Media, Inc. are “the

people behind Expendables 3” referred to by PIA.

58. PIA’s employee Caleb Chen publishes articles on PIA’s website advocating use of the PIA VPN service for piracy.

59. In 2020, Caleb Chen published an article on the PIA website entitled “Popular torrenting site YTS provides IP address logs to copyright lawyers to extort you with” to warn PIA end users and stated within his article “...for non Indian users of YTS, it seems like a pretty damn good idea [to use a VPN].”

When trying to torrent privately is bad enough, knowing that your logs will actually be given up to copyright infringement lawyers and end up being used against you in legal proceedings is a real life and ongoing worst case scenario for torrenters around the world. These sites are really a point of vulnerability for torrenters, both in terms of functionality and apparently liability. Many governments seek to block torrent sites – though countries like [India have confirmed that visiting a blocked torrent site with the use of a VPN is not illegal](#). In fact, for non Indian users of YTS, it seems like a pretty damn good idea.

The post [Popular torrenting site YTS provides IP address logs to copyright lawyers to extort you with](#) appeared first on [Privacy News Online by Private Internet Access VPN](#).

C. Non-Parties

60. Choopa is a US based host provider that, upon information and belief, provides US IP addresses and servers to Defendant.

61. Sharktech is US based host provider that, upon information and belief,

provides US IP addresses and servers to Defendant.

62. M247 is a foreign based host provider that, upon information and belief, provides US IP addresses and servers to Defendant.

63. Because of the nature of Defendant's operations, Plaintiffs cannot ascertain all IP addresses used by Defendant and thus the entire scope of Defendant's infringing activities. However, Defendant is in possession of the IP addresses that were assigned to them from their host providers. Plaintiff believes that information obtained in discovery will lead to the identification of IP address where Works of theirs or of affiliated entities were infringed and permit the Plaintiffs to identify the IP addresses and times where many of their Works were infringed thousands of times and to amend this Fourth Amended Complaint to join these entities as Plaintiffs. Plaintiff further believes that the information obtained in discovery may lead to the identification of additional infringing parties to be added to this Fourth Amended Complaint as Defendants. Plaintiffs will seek to amend this Fourth Amended Complaint to include the proper names and capacities once determined.

V. JOINDER

64. Pursuant to Fed. R. Civ. P. 20(a)(1), each of the Plaintiffs are properly joined because, as set forth in detail above and below, the Plaintiffs assert: (a) a right to relief arising out of the same transaction, occurrence, or series or transactions, namely (i) the use of host providers' services such as Sharktech and M247 by Defendant for contributing to infringements of the copyrights in Plaintiffs' Works and DMCA violations, and (ii) there are common questions of law and fact.

VI. FACTUAL BACKGROUND

A. The Plaintiffs Own the Copyrights to the Works

65. The Plaintiffs are the owner of the copyrights in the motion pictures (“Works”) as shown in Exhibit “1”. The Works are the subjects of copyright registrations, and this action is brought pursuant to 17 U.S.C. § 411.

66. The Plaintiffs are the owners of the copyrights by virtue of original authorship, assignment and/or company reorganization.

67. The Works are motion pictures currently offered for sale in commerce.

68. Defendant had notice of Plaintiffs’ rights through at least the credits indicated in the content of the motion pictures which bore proper copyright notices.

69. Defendant also had notice of Plaintiffs’ rights through general publication and advertising associated with the motion pictures, and packaging and copies, each of which bore a proper copyright notice.

70. Defendant also had notice of Plaintiffs’ rights through notices that were sent to it from its host providers such as Sharktech.

71. Defendant PIA also had notice of Plaintiffs’ rights through a subpoena that was served on it on 10/25/2018 by Plaintiff Venice PI, LLC in Civil Action No. 18-cv-192 (“The ShowBox lawsuit”) in the District of Hawaii concerning infringing activity at IP address 173.239.236.38.

72. PIA also had notice of Plaintiffs’ rights through a subpoena that was served on it on 1/17/2020 by Plaintiff Venice PI, LLC in Civil Action No. 19-cv-169 (“The YTS lawsuit”) in the District of Hawaii concerning infringing activity at IP address

91.207.175.82.

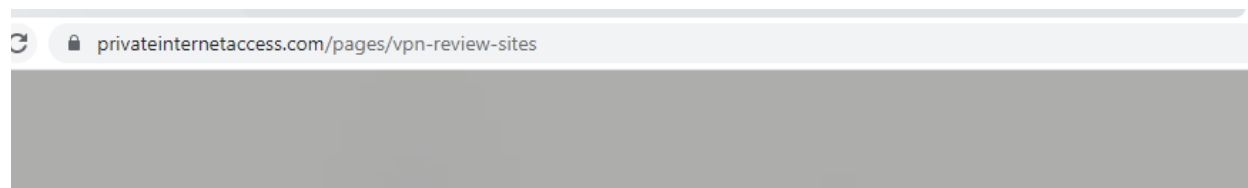
73. Indeed, thereafter Caleb Chen of PIA published an article warning its end users that Plaintiffs' counsel had obtained user logs from the piracy website YTS in the YTS lawsuit.

74. PIA also had notice of Plaintiffs' rights through a subpoena that was served on it in Civil Action No. 20-cv-3170-PAB-NRN in the District of Colorado concerning infringing activity at IP addresses 194.59.251.68 and 193.37.252.19.

B. Defendant and its end users Infringe Plaintiffs' Copyrights.

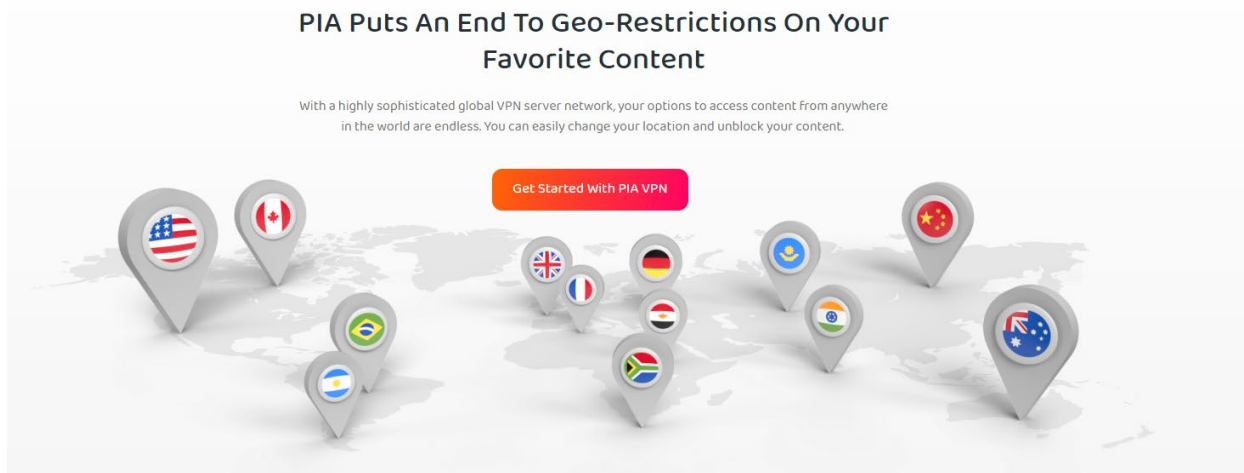
75. Defendant advertises the VPN service for allowing end users to bypass regional restrictions of streaming platforms to stream copies of copyright protected content including Plaintiffs' Works from locations Plaintiffs have not authorized the platform to stream the Works.

76. Defendant PIA advertises its VPN service for allowing its end users to "unblock Netflix USA".

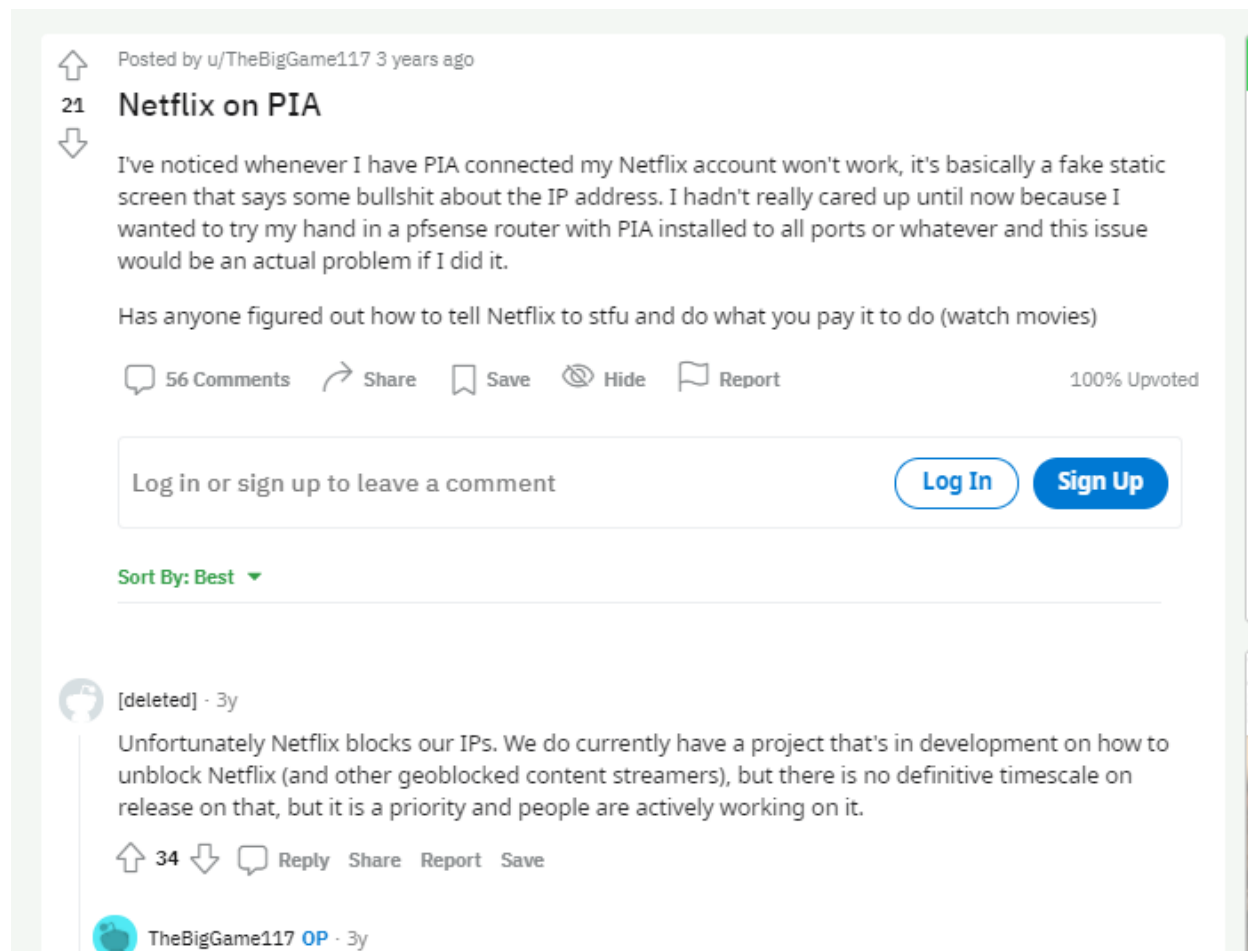


"Private Internet Access (PIA) is one of the leading VPN service providers, specializing in encrypted tunnels with several levels of security, offering an affordable alternative to pricey premium VPNs. It is fast and safe enough, allowing to unblock Netflix USA and download torrents on all the servers. Besides, it follows the no-logs policy."

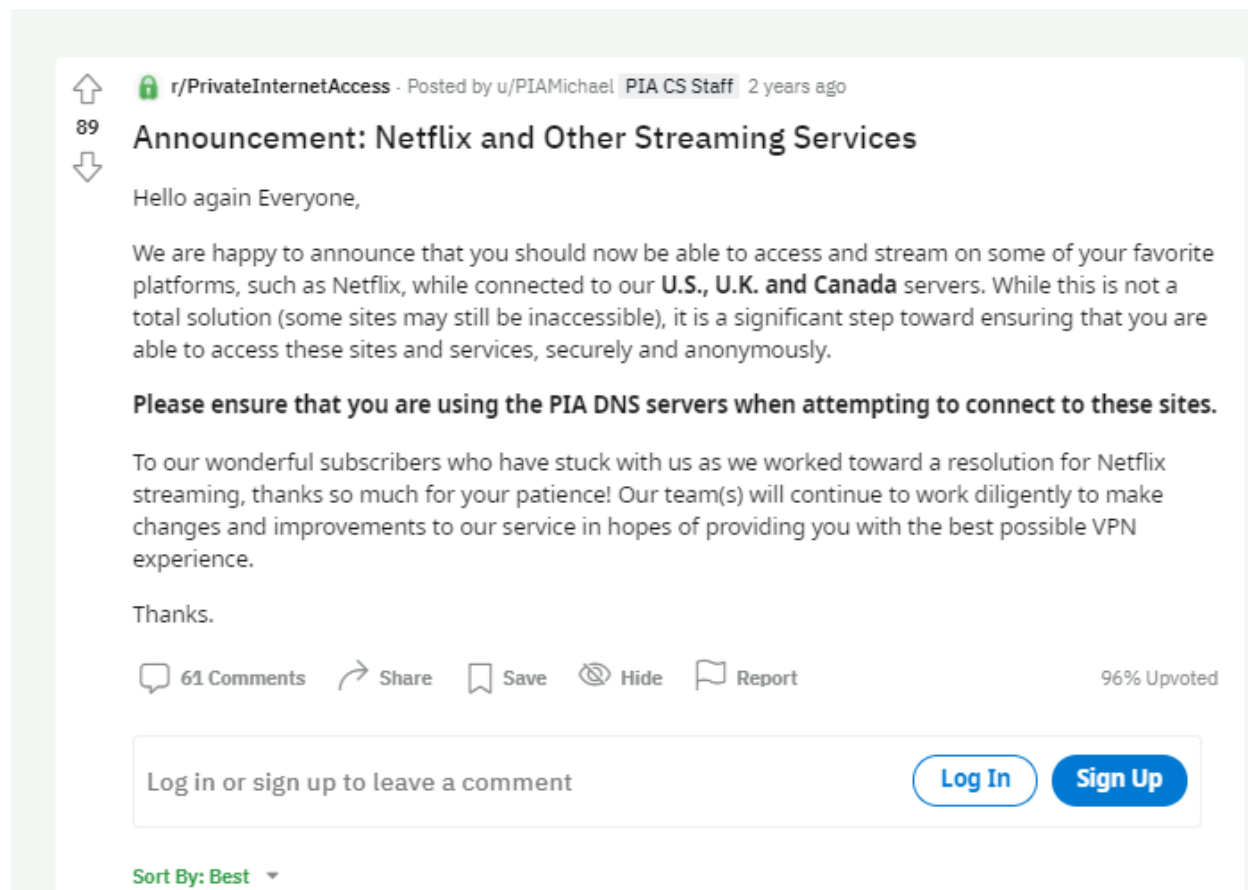
77. PIA states that its VPN service “Puts An End To Geo-Restrictions On Your Favorite Content.” <https://www.privateinternetaccess.com/unblock-websites-vpn> [last accessed on 11/4/2021].



78. PIA even stated in a Reddit forum that it was working on a project to unblock Netflix. See https://www.reddit.com/r/PrivateInternetAccess/comments/8s2z6h/netflix_on_pia/ [last accessed on 11/4/2021].



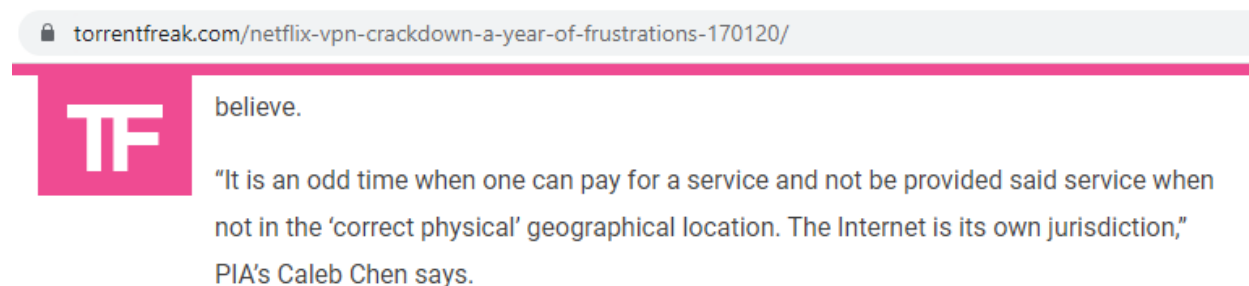
79. In 2019, PIA announced that it had secured a means for its end users to access Netflix from its “U.S., U.K. and Canada servers.” https://www.reddit.com/r/PrivateInternetAccess/comments/ddc6w4/announcement_netflix_and_other_streaming_services/ [last accessed on 11/4/2021].



80. Many legal platforms such as Netflix will “blacklist” IP addresses of known VPN providers to prevent violation of geographic restrictions. See Jacoby Parker, How does Netflix detect and block VPN use?, Aug. 16, 2021 <https://www.techradar.com/vpn/how-does-netflix-detect-and-block-vpn-use> [last accessed on 10/23/2021]. Accordingly, VPN providers such as Defendant have an incentive to not publicly reveal the IP addresses assigned to them so that they are not blacklisted and their end users prevented from streaming or distributing content from unauthorized regions.

81. When Netflix begin blacklisting IP addresses of VPN providers, Defendant PIA’s Caleb Chen criticized this practice and stated that “The Internet is its own

jurisdiction”. <https://torrentfreak.com/netflix-vpn-crackdown-a-year-of-frustrations-170120/> [last accessed on 11/18/2021].



82. Defendant and its customers (“end users”) use BitTorrent and BitTorrent Client applications such as Popcorn Time to infringe Plaintiffs’ exclusive rights of reproduction and distribution.

83. The United States Trade Representative (“USTR”) placed Popcorn Time on a list of examples of Notorious Markets engaged in and facilitating substantial piracy. See USTR, 2020 Review of Notorious Markets, Jan. 14, 2021, pg. 26, Available at [https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20\(final\).pdf](https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20(final).pdf) [last accessed on March 5, 2021].

84. Defendant distributes Plaintiffs’ Works in violation of Plaintiffs’ exclusive right of distribution.

85. Defendant distributes Plaintiffs’ Works for their end users in violation of Plaintiffs’ exclusive right of distribution.

86. Defendant reproduces Plaintiffs’ Works in violation of Plaintiffs’ exclusive right of reproduction.

87. Defendant reproduces Plaintiffs' Works for their end users in violation of Plaintiffs' exclusive right of distribution.

1. Defendant and its end users use BitTorrent to engage in piracy.

88. BitTorrent is one of the most common peer-to-peer file sharing protocols (in other words, set of computer rules) used for distributing large amounts of data.

89. The BitTorrent protocol's popularity stems from its ability to distribute a large file without creating a heavy load on the source computer and network. In short, to reduce the load on the source computer, rather than downloading a file from a single source computer (one computer directly connected to another), the BitTorrent protocol allows users to join a "swarm" of host computers to download and upload from each other simultaneously (one computer connected to numerous computers).

90. In a report from January 2011, a survey conducted by the firm Envisional estimated that 11.4 percent of all Internet traffic involved the unauthorized distribution of non-pornographic copyrighted content via BitTorrent.

91. A more recent study by Sandvine determined that file-sharing accounts for 3 percent of global downstream and 22 percent of upstream traffic, with 97% of that traffic in turn being BitTorrent. See Sandvine, "The Global Internet Phenomena Report", October 2018, <https://www.sandvine.com/hubfs/downloads/phenomena/2018-phenomena-report.pdf> [last accessed on May 27, 2021].

92. BitTorrent is overwhelmingly used for piracy. See David Price, "NetNames Piracy Analysis: Sizing the Piracy Universe", September 2013, pg. 18, http://creativefuture.org/wp-content/uploads/2016/01/netnames-sizing_piracy_universe-

[FULLreport-sept2013.pdf](#) [last accessed on Oct. 1, 2021] (“Of all unique visitors to bittorrent portals in January 2013, it is estimated that 96.28% sought infringing content during the month...”)

2. *The Initial Seed, Torrent, Hash and Tracker*

93. A BitTorrent user that wants to upload the new file, known as an “initial seeder,” starts by creating a “torrent” descriptor file using, for example, the Client he or she installed onto his or her computer.

94. The initial user or seeder of a file used a process referred to as “ripping” to create a copy of motion pictures from either Blu-ray or legal streaming services.

95. The initial seeder often modifies the file title of the Work to include a wording such as “TGx”, “FGT”, “RARBG” or “YTS” in the title of the torrent files and file copies in order to enhance a reputation for the quality of his or her torrent files and attract users to his or her piracy website.

96. The Client takes the target computer file, the “initial seed,” here the copyrighted Work, and divides it into identically sized groups of bits known as “pieces.”

97. The Client then gives each one of the computer file’s pieces, in this case, pieces of the copyrighted Works, a random and unique alphanumeric identifier known as a “hash” and records these hash identifiers in the torrent file.

98. When another peer later receives a particular piece, the hash identifier for that piece is compared to the hash identifier recorded in the torrent file for that piece to test that the piece is error-free. In this way, the hash identifier works like an electronic fingerprint to identify the source and origin of the piece and that the piece is authentic and

uncorrupted.

99. Torrent files also have an "announce" section, which specifies the URL (Uniform Resource Locator) of a "tracker," and an "info" section, containing (suggested) names for the files, their lengths, the piece length used, and the hash identifier for each piece, all of which are used by Clients on peer computers to verify the integrity of the data they receive.

100. The "tracker" is a computer or set of computers that a torrent file specifies and to which the torrent file provides peers with the URL address(es).

101. The tracker computer or computers direct a peer user's computer to other peer user's computers that have particular pieces of the file, here the copyrighted Work, on them and facilitates the exchange of data among the computers.

102. Depending on the BitTorrent Client, a tracker can either be a dedicated computer (centralized tracking) or each peer can act as a tracker (decentralized tracking.)

3. Torrent Sites

103. "Torrent sites" are websites that index torrent files that are currently being made available for copying and distribution by people using the BitTorrent protocol. There are numerous torrent websites including torrentgalaxy and the notorious YTS and RARBG websites.

104. The YTS and RARBG websites were noted by the USTR as examples of Notorious Markets defined as an online marketplace reportedly engaged in and facilitating substantial piracy. See USTR, 2014 Out-of-Cycle Review of Notorious Markets, Mar. 5, 2015, pg. 17, Available at

https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published_0.pdf [last accessed on May 7, 2021]; see also USTR, *2018 Out-of-Cycle Review of Notorious Markets*, April 2019, pgs. 24, 27 Available at https://ustr.gov/sites/default/files/2018_Notorious_Markets_List.pdf [accessed on May 7, 2021].

105. PIA recommends that individuals use VPN services such as its when using YTS to download torrent files to avoid Plaintiffs' counsel.

4. End users access the torrent sites from Sharktech IP addresses

106. End users accessed torrent sites including the YTS website to upload and download Plaintiffs' copyrighted Work from IP addresses provided by Defendant, which Defendant received from host providers such as Sharktech in Denver.

107. The IP address used by the end users then becomes a link to the infringing copies of Plaintiffs' Works.

108. End user Robert O'Brien (an end user of Defendant PIA) accessed the torrent website YTS from IP address 174.128.226.10 in Denver and downloaded torrent files for Plaintiffs' Work *Angel Has Fallen* and *Distorted*. See Decl. of Robert O'Brien at ¶¶2-3, 6.

109. End user Harry Beasor (an end user of Defendant PIA) accessed the torrent website YTS from IP address 91.207.175.82 and downloaded torrent files for Plaintiffs' Work *London Has Fallen* and *Mechanic: Resurrection*. See Aff. of Harry E. Beasor at ¶7.

110. End user Bryan Deem (an end user of Defendant PIA) accessed the torrent website YTS from IP address 193.37.252.37 and downloaded torrent files for Plaintiffs'

Works *The Hitman's Bodyguard* and *The Last Full Measure*. See Decl. of Bryan Deem at ¶2.

111. End user Brandon Brady (an end user of Defendant PIA) accessed the torrent website YTS from IP address 212.103.49.162 and downloaded torrent files for Plaintiff's Work *The Last Full Measure*. See Decl. of Brandon Brady at ¶2.

112. End user Cassandra Luker (an end user of Defendant PIA) accessed the torrent website YTS from IP address 199.116.115.143 and downloaded torrent files for Plaintiff's Work *London Has Fallen*. See Decl. of Cassandra Luker at ¶¶2-3.

113. End user Beth Wiecher (an end user of Defendant PIA) accessed the torrent website YTS from IP address 173.244.44.69 and downloaded a torrent file for Plaintiff's Work *London Has Fallen*. See Decl. of Beth Wiecher at ¶¶2-3.

114. End User Dale Powers (an end user of Defendant PIA) accessed the torrent website YTS from IP address 193.37.252.19 and downloaded a torrent file for Plaintiff's Work *Angel Has Fallen*. See Decl. of Dale Powers at ¶¶2-4.

5. The Peer Identification

115. The BitTorrent Client will assign an identification referred to as a Peer ID to the computer so that it can share content (here the copyrighted Work) with other peers. The Peer ID incorporates the IP address of the BitTorrent swarm participant.

6. Uploading and Downloading a Work Through a BitTorrent Swarm

116. Once the initial seeder has created a torrent and uploaded it onto one or more torrent sites, then other peers begin to download and upload the computer file to which the torrent is linked (here the copyrighted Work) using the BitTorrent protocol and

BitTorrent Client that the peers installed on their computers.

117. The BitTorrent protocol causes the initial seeder's computer to send different pieces of the computer file, here the copyrighted Work, to the peers seeking to download the computer file. Defendant transmits the pieces to the peers.

118. Once a peer receives a piece of the computer file, here a piece of the copyrighted Work, it starts transmitting that piece to the other peers. Defendant's end users transmit the pieces to the peers.

119. In this way, all of the peers and seeders are working together in what is called a "swarm."

120. Here, Defendant and its end users participated in a swarm and directly interacted and communicated with other members of the swarm through digital handshakes, the passing along of computer instructions, uploading and downloading, and by other types of transmissions, Plaintiffs' Works.

121. Defendant distributed its end users' transmissions to other members of the swarm.

122. In this way, and by way of example only, one initial seeder can create a torrent that breaks a movie up into hundreds or thousands of pieces saved in the form of a computer file, like the Works here, upload the torrent onto a torrent site, and deliver a different piece of the copyrighted Work to each of the peers. The recipient peers then automatically begin delivering the piece they just received to the other peers in the same swarm.

123. Once a peer has downloaded the full file, the BitTorrent Client reassembles

the pieces and the peer is able to view the movie. Also, once a peer has downloaded the full file, that peer becomes known as “an additional seed,” because it continues to distribute the torrent file, here the copyrighted Work.

7. The Plaintiffs’ Computer Investigator Identified Defendant’s IP Addresses as Participants in Swarms That Were Distributing Plaintiffs’ Copyrighted Works.

124. Sharktech and M247 reassigned IP addresses to Defendant.

125. Choopa reassigned IP addresses to Defendant PIA.

126. The Plaintiffs retained Maverickeye UG (“MEU”) to identify the IP addresses that are being used by those people that are using the BitTorrent protocol and the Internet to reproduce, distribute, display or perform the Plaintiffs’ copyrighted Works.

127. MEU used forensic software to enable the scanning of peer-to-peer networks for the presence of infringing transactions.

128. MEU extracted the resulting data emanating from the investigation, reviewed the evidence logs, and isolated the transactions and the IP addresses associated therewith for the files identified by the SHA-1 hash value of the Unique Hash Number.

129. The IP addresses, Unique Hash Numbers, and hit dates contained in Exhibit “2” accurately reflect what is contained in the evidence logs.

130. The logged information such as, for example, in Exhibit “2” shows that Defendant and/or Defendant’s end users distributed copies of the Plaintiffs’ copyrighted Works identified by the Unique Hash Number.

131. Defendant and/or its end users' computers used the IP addresses to connect to the investigative server from a computer (including one in this District at Sharktech's Denver facility as shown in Exhibit "2") in order to transmit a full copy, or a portion thereof, of a digital media file identified by the Unique Hash Number through networks (such as of Sharktech's) controlled by Defendant.

132. MEU's agent analyzed each BitTorrent "piece" distributed by the IP addresses listed and verified that re-assembly of the pieces using a BitTorrent Client results in a fully playable digital motion picture of the Works.

133. MEU's agent viewed the Works side-by-side with the digital media file that correlates to the Unique Hash Number and determined that they were identical, strikingly similar or substantially similar.

C. The Operator of the YTS website confirmed that the Defendant's end users downloaded torrent files for copying the Work from the YTS website.

134. The YTS website operator maintained records of activity of registered user accounts for IP addresses associated with data centers used by Defendant such as Choopa, M247 and Sharktech. See Exhibit "3" (Sharktech YTS users) at pg. 10 (Certificate of Authenticity).

135. The YTS website operator maintained records of activity of registered user accounts. See Exhibit "3" at pg. 10 (Certificate of Authenticity).

136. As shown in Exhibit "3", the records including the email address of the registered user account, the torrent files the registered account downloaded, the IP address from where the registered user accessed the YTS website, and the time.

137. The records show end users downloaded the torrent file for reproducing the Work, the same file copy MEU's agent verified that re-assembly of the pieces using a BitTorrent Client results in a fully playable digital motion picture of the Works, from IP addresses assigned to Sharktech and in Denver, CO.

D. Defendant and its end users reproduced and distributed copies of Plaintiffs' Works.

138. Defendant and/or its end users distributed at least pieces of each of Plaintiffs' Works over network connections to other peers in the Swarm.

139. Defendant and/or its end users reproduced at least pieces of each of Plaintiffs' Works within said network connections to distribute to the other peers in the Swarm.

140. End user Robert O'Brien (an end user of Defendant PIA) from IP address 174.128.226.10 in Denver distributed copies of Plaintiffs' Work *Angel Has Fallen* by the file name *Angel Has Fallen (2019) [WEBRip] [720p] [YTS.LT]* and *Distorted* by the file name *Distorted (2018) [BluRay] [720p] [YTS.AM]*. See Decl. of Robert O'Brien at ¶¶2-3, 6.

141. End user Harry Beasor (an end user of Defendant PIA) from IP address 91.207.175.82 distributed copies of Plaintiffs' Work *London Has Fallen* and *Mechanic: Resurrection*. See Aff. of Harry E. Beasor at ¶7.

142. End user Bryan Deem (an end user of Defendant PIA) from IP address 193.37.252.37 distributed copies of Plaintiffs' Works *The Hitman's Bodyguard* and *The Last Full Measure*. See Decl. of Bryan Deem at ¶2.

143. End user Brandon Brady (an end user of Defendant PIA) from IP address 212.103.49.162 distributed copies of Plaintiff's Work *The Last Full Measure*. See Decl. of Brandon Brady at ¶¶2.

144. End user Cassandra Luker (an end user of Defendant PIA) from IP address 199.116.115.143 distributed copies of Plaintiff's Work *London Has Fallen*. See Decl. of Cassandra Luker at ¶¶2-3.

145. Defendant PIA exported a copy of the Work to Australia when Cassandra Luker downloaded a copy of the Work and also imported a copy of the Work to United States from Australia when Cassandra Luker distributed a copy of the Work.

146. End user Beth Wiecher (an end user of Defendant PIA) from IP address 173.244.44.69 distributed copies of Plaintiff's Work *London Has Fallen*. See Decl. of Beth Wiecher at ¶¶2-3.

147. End user Dale Powers (an end user of Defendant PIA) from IP address 193.37.252.19 distributed copies of Plaintiff's Work *Angel Has Fallen*. See Decl. of Dale Powers at ¶¶2-4.

148. Defendant PIA exported a copy of the Work to Australia when Dale Powers downloaded a copy of the Work and also imported a copy of the Work to United States from Australia when Dale Powers distributed a copy of the Work.

149. Each IP address is a numerical identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication and permits devices to be identified and interface on the Internet and provides the location of the device in the network.

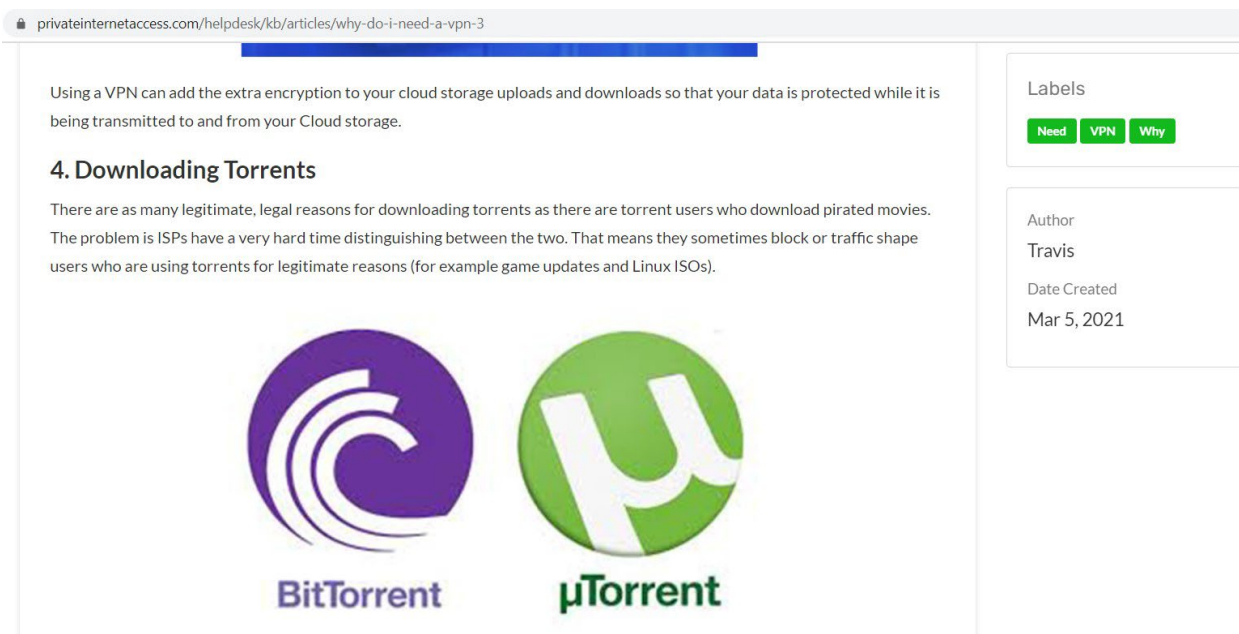
150. The IP addresses Defendant provides are indexes, references, pointers, and/or hypertext links that linked swarm participant to online locations such as Sharktech’s own servers in Denver and/or the end user’s computers containing unauthorized copies of Plaintiffs’ Works or sources for distributing Plaintiffs’ Works.

E. Defendant intentionally induces piracy of copyright protected Works including Plaintiffs’.

151. Defendant obtained services such as IP addresses and servers from host providers such as Sharktech for the purpose of infringing copyright protected Works including Plaintiffs’.

152. Defendant promotes its services for the purpose of infringing copyright protected Works including Plaintiffs’ (i.e. – piracy).

153. Defendant PIA acknowledges that its end users use its VPN service for piracy.



154. PIA instructs its users how to *optimize* use of its VPN service for piracy.

privateinternetaccess.com/helpdesk/kb/articles/how-do-i-enable-port-forwarding-on-my-vpn-2

Help Center > Knowledgebase > Technical > Browsing and Internet > Torrents > How do I enable port forwarding on my VPN?

How do I enable port forwarding on my VPN?

TH
Last updated: Mar 5, 2021 by Travis Hackbarth

The Port Forwarding option in our Windows, Mac, Linux and Android software can be used to potentially optimize torrent performance.

Enable Port Forwarding:

In order to enable port forwarding in our PIA app, first disconnect from the VPN. Right-click the PIA Tray icon and select "Settings". From within the settings, select the Network tab and check the "Request Port Forwarding" checkbox. You will now see, in the server list, the servers on which you can connect with port-forwarding enabled. Any server that is unavailable, will be blacked out. At the moment, all of our non US Servers offer port-forwarding functionality and you can find a list of all of the servers we offer, here: <https://www.privateinternetaccess.com/pages/network/>

Locating Forwarded Port

Once connected to on one of these port forwarding gateways, please open the application. From within the application you will see the forwarded port just below the VPN IP address.

Subscribe

Labels
Port Forwarding

Author
Travis

Date Created
Mar 5, 2021

155. PIA warned its end users that Plaintiffs' counsel had obtained log information for users of the piracy website YTS after it received a subpoena in that case.

156. PIA's parent company and alter ego Kape promotes PIA's VPN service for piracy on its website.

157. Kape warns that "Risks of Torrenting in the US" include "Copyright trolls... that locate and penalize users who download copyrighted content." <https://www.vpnmentor.com/blog/downloading-torrents-in-the-u-s/> [last accessed on 11/5/2021].

What Are the Risks of Torrenting in the US

Torrenting in the US can present some serious challenges. On top of legal risks, there are various cyber threats you are vulnerable to whenever you torrent in the US. Find out more about the 3 major risks of torrenting below.

Copyright trolls

Copyright trolls are companies that locate and penalize users who download copyrighted content. They're usually third parties, hired to act on behalf of big movie studios and music labels. Copyright trolls use deep packet inspection (DPI) to track your downloads and visited sites. Once they find someone downloading illegal files, they hand out a settlement letter that can sometimes come with fines of up to \$100K. The team at vpnMentor doesn't condone illegal torrenting, but even if you didn't download copyrighted content intentionally and only did it by accident, you'd be exposing yourself to copyright trolls.

158. Kape states that PIA's kill switch is great for protecting users that want to pirate. <https://www.vpnranks.com/reviews/private-internet-access/> [last accessed on Nov. 4, 2021] ("I'd recommend users to keep the Kill Switch enabled at all times, especially if you're performing sensitive tasks like downloading torrents in a country with strict laws against online piracy").

PIA VPN Kill Switch

The PIA VPN Kill Switch disconnects your internet if you lose your VPN connection for one reason or the other. This stops your actual IP address from getting exposed to your local ISP or the site you are visiting.

I'd recommend users to keep the Kill Switch enabled at all times, especially if you're performing sensitive tasks like downloading torrents in a country with strict laws against online piracy.

The Kill Switch will ensure that your real identity remains hidden even in case of sudden connection interruptions.

Encrypted Wi-Fi

What makes PIA a standout VPN service from its competitors is its encrypted Wi-Fi feature. When you use Private Internet Access on your Wi-Fi, it protects the device through WPA protocol first. Therefore, you have to provide an authentication key before using the VPN on Wi-Fi devices, which makes your connection sessions more secure.

PIA SOCKS5 Proxy

PIA SOCKS5 proxy offers an **additional layer of authentication** as it only allows authorized users when it comes to accessing the servers. In addition, it provides an appreciable connection speed as compared to other protocols.

This makes SOCKS5 good for purposes such as downloading and streaming. The popular usage of the protocol involves downloading torrents because it usually results in faster speeds.

However, it must be remembered that if you're in a country with strict laws against torrenting, the wiser decision would be to stick to more secure protocols like OpenVPN even if it results in slightly slower speeds. This is because SOCKS5 has weaker security as compared to other VPN protocols.

159. Kape states here that “The safest way to torrent in the US is by using a VPN” and recommends Private Internet Access and ExpressVPN because each “Works with: The Pirate Bay, RARBG, 1337x, YTS, Netflix, Hulu...and more”.

1. ExpressVPN — Highly Secure With Fast Speeds for Torrenting in the US



Try ExpressVPN >




- ✓ Strict zero-logs policy, military-grade 256-bit encryption, and an automatic kill switch to protect your privacy while torrenting in the US
- ✓ Unlimited data and lightning-fast speeds to torrent in the US without lag
- ✓ A vast network of P2P servers that allow you to torrent from anywhere
- ✓ 5 simultaneous device connections
- ✓ 30-day money-back guarantee
- ✓ Works with: The Pirate Bay, RARBG, 1337x, YTS, Netflix, Hulu, HBO Max, and more
- ✓ Compatible with: Windows, Mac, iOS, Android, Linux, routers, and more

4. PIA — P2P-Supporting Servers for Fast Torrenting in the US



Try Private Internet Access >

- ✓ No-logs policy, AES 256-bit encryption, and an automatic kill switch to keep you secure while you torrent in the US
- ✓ Unlimited data and decent speeds to torrent in the US without buffering
- ✓ 29,650 servers in 70 countries, with most locations offering P2P support
- ✓ 10 simultaneous device connections
- ✓ 30-day money-back guarantee
- ✓ Works with: The Pirate Bay, RARBG, 1337x, YTS, Netflix, HBO Now, and more
- ✓ Compatible with: Mac, Windows, Linux, Android, iOS, and more

 **November 2021 Update:** PIA doesn't usually have deals or discounts (it's already so affordable), but right now you can [get a new subscription for a crazy 84% off!](#)

160. PIA's parent company and alter ego Kape promotes ExpressVPN's VPN service for using the piracy app "ShowBox". See <https://www.vpnmentor.com/blog/is-showbox-safe-it-is-but-only-if-you-do-this/> [last accessed on 11/4/2021].

161. Here Defendant PIA's parent company Kape acknowledges that ShowBox is "illegal in most Western countries" and that "There is also a risk that Hollywood studios...in litigation against...Showbox could actually sue end users....You can insulate yourself from these risks by using a VPN..."

Is Showbox Legal?

Showbox, which is considered to have mostly pirated content, is **illegal in most Western countries** with strict intellectual property and copyright laws.

However, there is a gray area for users. **In many cases, streaming pirated content online is considered legal**, even if the website in question does not own the pertinent copyright or licensing. What is almost universally considered illegal is downloading pirated content to your own device.

There is also a risk that Hollywood studios or TV producers in litigation against websites offering Showbox could actually **sue end users**. Some of these websites now warn users that their **IP addresses and browsing history could be made available** to interested parties through their ISP.

You can insulate yourself from these risks by using a VPN. **VPNs prevent ISPs from being able to view your online activity or personal data** and passing it on to third parties such as studios, producers, and law firms.

VPNs also allow you to bypass the geo-restrictions that some countries use to block Showbox, allowing you to get through to the service's servers and the content you want to watch.

162. Indeed, some of the Plaintiffs in this action joined other rightsholders and filed a lawsuit against operators of the ShowBox app and websites that promoted ShowBox app in the District of Hawaii (1:18-cv-192). Plaintiffs served a subpoena on Defendant PIA concerning the operator of the ShowBox's use of PIA's VPN service.

163. Plaintiffs' investigator, Eric Smith, confirmed that Showbox can be used to download, reproduce, and distribute copies of copyright protected Works such as "I Feel Pretty" and "Hunter Killer" exactly as promoted and encouraged by Defendant.

164. Defendant PIA's parent company and alter ego Kape promotes ExpressVPN's VPN service promotes as "reliable" torrent sites: The Pirate Bay; YTS; 1337x; RARBG and Limetorrents for the user to use after the users has gotten "a reputable VPN" with "military-grade encryption and hides your IP address". The military-grade language include a link to the ExpressVPN website. <https://www.vpnmentor.com/blog/torrent-beginners-bittorrent-explained/> [last accessed

on 11/5/2021].

Step 6: Download a safe torrent

Downloading a safe torrent is crucial because the wrong one can be filled with malware. Hackers usually fill torrents with malware and disguise them to wreak havoc. Therefore, **make sure you only download torrents that have been verified for safety**.

A good place to start is to **use a trustworthy torrent site that's well established**. **Don't download a torrent from an obscure site that you found off a Google search**, as Google often displays the URLs of fake sites.

Some reliable torrent sites include:

- The Pirate Bay
- YTS
- 1337x
- RARBG
- Limetorrents

165. Defendant PIA's parent company and alter ego Kape promotes ExpressVPN's VPN service for using the piracy apps and piracy websites such as "MoviesJoy", "Popcorn Time" "SubsMovies". See <https://www.vpnmentor.com/blog/best-alternatives-to-flixtor-get-free-movies-tv/> [last accessed on 11/4/2021].

166. Here Defendant PIA's parent company and alter ego Kape warns its readers to use a VPN to make it "nearly impossible" to get caught infringing copyrights.

Protection from Legal Consequences of Copyright Violations

It's perfectly **legal to watch a video on a website that has secured rights to distribute it**. However, if the website is not authorized to show the video, you could get pulled into legal battles over copyright infringement.

By encrypting your traffic and **masking your IP address, VPNs make it nearly impossible for anyone to trace your online activity back to you**. So even if the streaming website gets in trouble for violating copyright laws, you won't.

167. Defendant PIA's parent company and alter ego Kape explicitly promotes notorious piracy website such as YTS, 1337x, RARBG and the Pirate Bay and states that ExpressVPN can be used to "...stop you from getting in trouble for torrenting if it's banned in your country or you accidentally download copyrighted material." <https://www.vpnmentor.com/blog/best-elitetorrent-alternatives/> [last accessed on 11/4/2021].

168. Defendant pays commissions to marketing affiliates that promote its VPN services for piracy.

169. Upon information and belief, Defendant pays these marketing affiliates a percentage of the subscription fee for each end user they refer that pays for a subscription for the VPN service.

170. Defendant's marketing affiliate "ProPrivacy" recommended PIA, CyberGhost and ExpressVPN as three of the top five VPNs "you will need to use...to torrent with YTS safely and avoid getting into trouble." <https://proprivacy.com/comparison/vpn-yts> [last accessed on 11/4/2021].



171. End users use Defendant’s VPN service exactly as explained and encouraged – to infringe copyright protected content while logged into the VPN service so they can conceal their illicit activities.

172. Defendant promotes its VPN service as a tool to engage in massive copyright infringement to entice end users to purchase its VPN service.

173. Based upon Defendant’s encouragement that the VPN service can be used to “safely” operate piracy apps such as Popcorn Time and visit torrent sites such as Pirate Bay, Kickass Torrents, YTS and Extratorrents and pirate, end users purchase the VPN service, install piracy apps such as Popcorn Time on their devices and/or visit torrent sites

to infringe copyright protected content including Plaintiffs' while using Defendant's VPN service.

174. Defendant has the capability to log its end users' access to their VPN service but purposely deletes the logged information so that it can promote the service as a means to pirate copyright protected Works anonymously.

175. Defendant also purposely deletes the logged information so that it can use the service as a means to pirate copyright protected Works anonymously.

176. Defendant interferes with standard technical measures used by copyright holders to identify or protect copyright works by purposefully deleted its and its end users' logged information. See 17 U.S.C. § 512(i)(1)(B).

177. Defendant specifically admits that it deleted the end users' logged information to protect the end users' piracy activities in promotions and advertisements. See e.g. Ernesto, "Which VPN Providers Really Take Privacy Seriously in 2021?", June 14, 2021, <https://torrentfreak.com/best-vpn-anonymous-no-logging/#tf-comments> [last accessed on Aug. 1, 2021] (In response to questions concerning BitTorrent activity, PIA states "We do not store any logs relating to traffic, session, DNS or metadata. There are no logs kept for any person or entity to match an IP address and a timestamp to a current or former user of our service. In summary, we do not log, period.")

178. Defendant does not have a safe harbor from liability because it has not "adopted and reasonably implemented...a policy that provides for the termination in appropriate circumstances of subscribers...who are repeat infringers." 17 U.S.C. § 512(i)(1)(A).

F. Defendant's subscribers knew the Copyright Management Information included in the files they distributed to other peers had been removed or altered without the authority of Plaintiffs.

179. A legitimate file copy of the Work includes copyright management information ("CMI") indicating the title.

180. The initial seeder of the infringing file copies of Plaintiff's Work added wording to the file titles to "brand" the quality of piracy files he or she released and attract further traffic to his or her website.

181. For example, the initial seeder of the infringing file copies of *Angel Has Fallen* added the wording "YTS" to the file titles to brand the quality of piracy files he or she released and attract further traffic to the YTS website.

182. For example, the initial seeder of the infringing file copies of *The Outpost* added the wording "TGx" to the file titles to brand the quality of piracy files he or she released and attract further traffic to the torrentgalaxy website.

183. The words YTS or TGx are not included in the file title of legitimate copies or streams of the Plaintiffs' Works. The initial seeders of the Work altered the title to falsely include the words such as "YTS" or "TGx" in the CMI.

184. The file copies Defendant distributed to other peers in the Swarm included the altered CMI in the file title.

185. Defendant's end users knew that TGx, FGT, YTS and RARBG were not the author of Plaintiffs' Works.

186. Defendant's end users knew that TGx, FGT, YTS and RARBG were not a

licensed distributor of Plaintiffs' Works. Indeed, the YTS website includes a warning to this effect.

187. Defendant's end users knew that the CMI that included TGx, FGT, YTS and RARBG in the file names was false.

188. Defendant's end users knew that the file copies of the Work that they distributed to other peers in the Swarm included the altered CMI without the authority of Plaintiffs.

189. Defendant's end users knew that the CMI in the title they distributed to other peers in the Swarm included the altered CMI without the authority of Plaintiffs.

190. Defendant's end users knew that the false or altered CMI in the titles would induce, enable, facilitate or conceal infringements of the Works when they distributed the false CMI, altered CMI or Works including the false or altered CMI.

191. Namely, Defendant's end users knew that other recipients would see the file titles and use the altered CMI to go to the website such as YTS from where the torrent files originated to obtain unlicensed copies of the Work.

192. Indeed, some of Defendant's end users have registered accounts with piracy website such as YTS.

193. By providing the website information in the altered CMI to others, Defendant's end users induced, enabled and facilitated further infringements of the Work.

194. Indeed, Defendant promotes its VPN services for accessing piracy website such as YTS and RARBG.

G. Defendant had knowledge that its end users were infringing Plaintiffs' Works

and distributing file copies of the Works with altered CMI and that the IP addresses it provided to the end users were links to infringing activity but continued to provide service to their end users

195. Plaintiffs engaged MEU to generate Notices of infringements (“Notices”) styled per 17 U.S.C. §512(c)(3) of the DMCA to be sent to service providers of IP addresses where MEU confirmed infringement of copyright protected content.

196. Each Notice included at least the name of the copyright owner, the title of the Work, the manner by which it was infringed, the infringing file name which includes the altered CMI, the IP address and port number at where infringement was confirmed and the time of infringement down to the second. See Exhibits “4” and “5” (excerpts below).

Protocol: BITTORRENT
Infringed Work: The Outpost
Infringing FileName: The.Outpost.2020.720p.GPLAY.WEBRip.900MB.x264-GalaxyRG[TGx]
Infringing FileSize: 940063994
Infringer's IP Address: 70.39.102.165
Infringer's Port: 52098
Initial Infringement Timestamp: 2021-02-10 00:11:17

Protocol: BITTORRENT
Infringed Work: The Hitmans Wifes Bodyguard
Infringing FileName: The.Hitmans.Wifes.Bodyguard.2021.EXTENDED.1080p.WEBRip.x265-RARBG
Infringing FileSize: 1942629641
Infringer's IP Address: 70.39.102.165
Infringer's Port: 49934
Initial Infringement Timestamp: 2021-07-25 06:10:02

197. MEU determines the proper abuse contact email address for the service provider assigned the IP addresses at issue from publicly available information from Whois records of

ARIN.

198. Plaintiffs' agent sends the Notice to the abuse contact email address for the host provider associated with the IP addresses.

199. Upon information and belief, the host provider forwarded these Notices to Defendant.

200. Upon information and belief, other rightsholders had similar Notices sent to host providers concerning infringing activity at IP addresses assigned to Defendant.

201. Just between March and September of this year, Plaintiffs' agent sent thousands of Notice to Sharktech confirming infringements of the motion pictures: 211; After We Collided; Angel Has Fallen; Automata; Ava; Before I Go to Sleep; Between Worlds; Blackbird; Boyka: Undisputed IV; Criminal; Dallas Buyers Club; Dead Trigger; Distorted; Disturbing the Peace; Extremely Wicked, Shockingly Evil and Vile; Hellboy; Homefront; Hunter Killer; I Am Wrath; I Feel Pretty; Jolt; Kill Chain; Lansky; Leatherface; London Has Fallen; Look Away; Mechanic: Resurrection; Olympus Has Fallen; Once Upon A Time in Venice; Rambo: Last Blood; Run Hide Fight; Shock and Awe; Singularity; SKIN; Speed Kills; Status Update; Survivor; Tesla; The 2nd; The Expendables 3; The Hitman's Bodyguard; The Hitman's Wife's Bodyguard; The Humbling; The Outpost; The Professor and the Madman; The Protégé; and Till Death.

202. For example, just between February and September of this year, Plaintiffs' agent sent Sharktech 1151 Notices concerning infringements of *Hitman's Wife's Bodyguard* at IP addresses Sharktech reassigned to PIA.

203. Upon information and belief, Sharktech forwarded each of the Notices to

dmca@privateinternetaccess.com and john@privateinternetaccess.com.

204. Plaintiffs' agent sent 12 Notices to Sharktech concerning infringement of movies such as *Kill Chain*, *Hitman's Bodyguard*, *The Outpost*, *The Hitman's Wife's Bodyguard*, and *London Has Fallen* between February and March of this year at IP address 70.39.108.195. Upon information and belief, Sharktech forwarded each of the Notices to dmca@privateinternetaccess.com and john@privateinternetaccess.com.

205. During this same period the PIA end user at IP address 70.39.108.195 shared multiple copies of these Works. For example, the end user was confirmed by MEU sharing copies of *The Hitman's Wife's Bodyguard* 21 times and *The Outpost* 14 times just between February and March of this year.

206. The host provider Choopa allocated to Defendant PIA IP addresses including 108.61.13.43; 108.61.13.44; 108.61.13.45 and 108.61.13.46 from 8/3/2012.

207. Between May 7, 2018 to the present, Plaintiffs' agent sent Choopa 247 Notices concerning infringement of Status Update; *The Hitman's Bodyguard*; *Day of the Dead*; 211; *Once Upon a Time in Venice*; *I Feel Pretty*; *The Mechanic: Resurrection*; *Criminal*; and *Automata* at these IP addresses that, upon information and belief, Choopa forwarded to Defendant PIA.

208. The host provider allocated to Defendant PIA IP addresses including 173.239.232.23 and 173.239.232.101.

209. Plaintiffs' agent sent hundreds of Notices to the host provider that, upon information and belief, forwarded the Notices to Defendant PIA.

210. In 2019, Defendant PIA and/or its end user distributed copies of *The Brass*

Teapot and *Lost Child* from IP addresses 173.239.232.89, 173.239.232.101 and 173.239.232.23 even after Plaintiffs' agent had sent hundreds of notices to the host provider concerning this IP address.

211. Defendant failed to terminate the accounts of its end users associated with these IP addresses or take any meaningful action in response to these Notices.

212. Defendant failed to even forward the Notices to its end users.

213. Plaintiff Venice PI, LLC served a subpoena on Defendant PIA in Civil Action No. 19-cv-169 in the District of Hawaii concerning infringing activity at IP address 91.207.175.82.

214. Plaintiff Millennium Funding, Inc. served a subpoena on Defendant PIA in Civil Action No. 20-cv-3170-PAB-NRN in the District of Colorado concerning infringing activity at IP addresses 193.37.252.19 and 194.59.251.68.

215. Defendant PIA failed to terminate the accounts of its end users associated with these IP addresses in the subpoena or take any meaningful action in response to these subpoenas.

216. In the contrary, PIA warned its end users that Plaintiffs' counsel had received log information from the notorious YTS piracy website.

217. Defendant could have taken simple measures to stop its end users from continuing to reproduce and/or distribute Plaintiffs' works but did not.

218. For example, Defendant could have temporarily "null-routed" the IP addresses to disable the link to the infringing activity and stop further piracy of Plaintiffs' works.

219. For example, Defendant could have temporarily suspended the end users' account to stop further piracy of Plaintiffs' works.

220. For example, Defendant could have blocked certain ports such as ports 6881-6889 that are used for BitTorrent.

221. If Defendant had even forwarded the Notices to its end users, the end user would likely have ceased the conduct. See Decl. of Robert O'Brien at ¶13 ("I would have immediately ceased...had I received any of these notices earlier or had my service been temporarily terminated."); Decl. of Tayah Durnan at ¶5("I would have immediately stopped...had I received any warning or notices...")

222. Defendant continued to provide service to its end users despite knowledge that its end users were using the service to engage and facilitate massive piracy of copyright protected Works including the Plaintiffs'.

223. Defendant purposefully failed to do anything about its end users' flagrant piracy including failing to even forward the Notices on to its end users because it was motivated to continue receiving payments from its end users and was concerned that its end users would cancel their service if it forwarded the notices to its end users.

H. Defendant controls the conduct of end users.

224. Defendant can terminate the accounts of its' end users at any time.

225. Upon information and belief, Defendant promptly terminates end user accounts when said end users failed to pay for the service.

226. Upon information and belief, Defendant blocks specific traffic it considers abusive.

I. Defendant does not have a safe harbor from liability.

227. As part of the DMCA, Congress created a safe harbor that limits the liability of a service provider for copyright infringement when their involvement is limited to, among other things, “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider.” 17 U.S.C. § 512(a). To benefit from this safe harbor, however, an ISP must demonstrate that it “has adopted and reasonably implemented...a policy that provides for the termination in appropriate circumstances of subscribers...who are repeat infringers.” 17 U.S.C. § 512(i)(1)(A).

228. Defendant does not have a policy of terminating repeat infringers.

229. Plaintiffs’ agents have sent thousands of Notices to host providers such as Sharktech concerning infringements at IP addresses the host providers reassigned to Defendant.

230. Despite these host providers forwarding the Notices to Defendant, Defendant failed to terminate the accounts and/or take any meaningful actions against its end users in response to these Notices consistent with a reasonably implemented policy for termination of subscribers and account holders of the service provider’s system or network who are repeat infringers necessary to support a safe harbor from liability (“policy”).

231. In many cases, Defendant was untruthful to the host providers when the host provider required a follow up response to the Notices.

232. Congress created a safe harbor that limits the liability of a service provider for copyright infringement “...by reason of the storage at the direction of a user of material

that resides on a system or network controlled or operated by or for the service provider, if the service provider” does not have the requisite knowledge, “...responds expeditiously to remove or disable access to, the material...” and has the appropriate designated agent for receiving notices. 17 U.S.C. § 512(c)(1), (2).

233. Defendant and/or its end users use IP addresses of Defendant as links to access infringing copies of Plaintiffs’ Works at Defendant’s servers.

234. The thousands of Notices Plaintiffs’ agent sent to Defendant’s host providers concerning infringements included information such as the IP addresses that were forwarded to Defendant could have been used by Defendant to disable access to the infringing material and/or activity.

235. Defendant failed to respond and expeditiously remove or disable access to the material and/or activity in response to the thousands of Notices Plaintiffs’ agent sent to their host providers such as Sharktech.

236. Defendant’s conduct renders it ineligible for safe harbor immunity from copyright liability under the DMCA.

J. The copyright infringements arise from Defendant’s advertisements.

237. Defendant advertises that it’s service can be used to do whatever end users wish since there are no logs.

238. Defendant’s end users are motivated to become customers from Defendant’s advertisements.

239. Defendant’s end users are motivated to become customers from the knowledge of Defendant’s practice of deleting logs, ignoring notices of infringements or

failing to take any meaningful action.

240. The ability and availability for Defendant's end users to distribute and stream copyright protected Works including Plaintiffs from servers and IP addresses controlled by Defendant while concealing their identity is a draw for end users and at least one of their motivations to become customers of Defendant.

241. Defendant directly profits from end users streaming and distribution of Plaintiffs' copyright protected Works without authorization.

K. Defendant PIA breached a settlement agreement with Plaintiffs.

242. On or about Sept. 1, 2021, Plaintiffs, other rightsholders and Defendant PIA entered into a settlement agreement ("Agreement") to resolve copyright claims in this action and other claims. See Exhibit "6".

243. Plaintiffs' counsel, counsel for Kape (Dr. Venetia Argyropoulou) and counsel for PIA negotiated the Agreement.

244. Counsel for PIA had authority to bind PIA.

245. Dr. Argyropoulou had authority to bind PIA.

246. The Agreement provided for PIA to make a payment to Plaintiffs and non-parties by Sept. 21, 2021.

247. In the Agreement PIA acknowledges that the Agreement "...does not give PIA any license to distribute for commercial uses or for any other purposes whatsoever, the Works owned by Owners."

248. The Agreement provides for being "governed by and construed in accordance with the laws of the State of Hawaii..."

249. One of the rightsholders in the Agreement is a Hawaii limited liability company.

250. On Sept. 1, 2021, the general counsel for PIA sent an email to Plaintiffs' counsel stating, "We are sending the approved version of the final settlement agreement after [general counsel of Kape Dr.] Venetia [Argyropoulou] sent her feedback and I made a couple of small revisions."

251. That same day, Plaintiffs' counsel replied with a revised version that merely changed "Voltage Pictures, Inc. to LLC" and changed payment due date from 8/15/2021 to 9/21/2021. Plaintiffs' counsel emphasized that "It is very important that the payment arrive before end of 9/30/2021."

252. That same day, general counsel for PIA stated that he was revising to make the signing party Moran Laufer (the CFO of PIA and Kape) rather than himself and sending over for his signature.

253. That same day, Plaintiffs' counsel replied to the general counsel for PIA "This is fine".

254. The general counsel for PIA never stated an intention not to be bound by the Agreement absent an executed writing.

255. The Agreement is a valid, binding and enforceable contract.

256. Plaintiffs' counsel also represents Plaintiffs in Civil Action 21-cv-643 in the E. District of Virginia. In preparing a First Amended Complaint in the Virginia action to name further Defendants, Plaintiffs' counsel for the first time became aware that an intended Defendant ZenGuard is also a subsidiary of Kape. Plaintiffs' counsel promptly

notified general counsel for PIA of its intentions in the Virginia action in the spirit of good faith.

257. Despite Plaintiffs and PIA agreeing to the fully enforceable Agreement, on Sept. 10, 2021 the general counsel for PIA sent a new proposed agreement to also release ZenGuard that replaced the name PIA with “Kape Technologies Plc (“:Kape” which such term shall also include all of KAPE TECHNOLOGIES PLC current and prospective subsidiaries)”, increased the total amount to be paid to settle claims for ZenGuard, and provided that Moran Laufer would be the signing party on behalf of Kape.

258. On Sept. 11, 2021 (Saturday) at 9:39 AM Hawaii Time, Dr. Argyropoulou suddenly emailed Plaintiffs’ counsel and demanded that he sign the new proposed agreement on behalf of the Plaintiffs by the next day within less than 14 hours (less than 9 hours when taking into account time zone of some of the Plaintiffs).

259. Plaintiffs’ counsel pointed out in reply that because it was Saturday morning (and afternoon in the mainland), it would be impossible to get in touch with his clients within less than 14 hours.

260. Dr. Argyropoulou threateningly replied that “...we fully intend to take all necessary legal measures to protect our brand names, if a settlement is not reached now.”

261. Plaintiffs’ counsel further pointed out in reply that the “current and prospective subsidiaries” language was vague and could potentially release a Defendant in other outstanding lawsuits if Kape purchased that Defendant.

262. Dr. Argyropoulou replied that she is “willing to limit this to prospective

subsidiaries not based in the US”.

263. Plaintiffs’ counsel then pointed out to Dr. Argyropoulou that “Many of the foreign VPN providers have also agreed to be subject to jurisdiction in the US just like ZenGuard.”

264. Less than two days later (Sept. 13, 2021), the news site CNet reported that Kape was purchasing ExpressVPN for \$936 million dollars. <https://www.cnet.com/tech/services-and-software/kape-technologies-buys-expressvpn-as-part-of-a-936-million-deal/> [last accessed on 11/5/2021].

265. At the time Dr. Argyropoulou demanded that Plaintiffs’ counsel sign the new proposed agreement, ExpressVPN was a Defendant in the Virginia action.

266. Upon information and belief, Dr. Argyropoulou was involved with Kape’s purchase of ExpressVPN. Accordingly, Dr. Argyropoulou knew that Kape was in the process of purchasing ExpressVPN when she demanded that Plaintiffs’ counsel sign the new proposed agreement within less than 14 hours.

267. PIA, through its agent Dr. Argyropoulou, breached the Agreement by attempting to deceive Plaintiffs’ counsel into signing the new proposed agreement on behalf of Plaintiffs in which she had snuck in a full release for ExpressVPN under the false pretenses of settling the PIA and ZenGuard matters.

268. PIA, through its agent Dr. Argyropoulou, breached the Agreement by attempting to strongarm Plaintiffs’ counsel to sign the new proposed agreement on behalf of Plaintiffs within less than 14 hours before its parent and alter ego Kape publicly released that it was purchasing ExpressVPN.

269. PIA purposefully and maliciously breached the Agreement to attempt to release its alter ego Kape's "prospective subsidiary not based in the US" ExpressVPN by attempting to sneak in vague language in a proposed new agreement and coerce Plaintiffs' counsel to sign the proposed new agreement on behalf of his clients by threatening him and giving him a ridiculous deadline of less than 14 hours on a Saturday.

270. PIA breached the covenant of good faith and fair dealing implied in the Agreement.

271. PIA acted wantonly, oppressively, or with such malice as implies a spirit of mischief or criminal indifference to its civil obligations.

272. PIA misconduct is willful and with conscious indifference to consequences.

273. Plaintiffs relied upon this Agreement to their detriment.

274. Plaintiffs sent PIA a 10-day notice to cure pursuant to ¶23 of the settlement agreement on 11/1/2021. PIA did not cure its breach.

275. Plaintiffs have substantially complied with the Agreement.

276. To the extent Plaintiffs have not complied with the Agreement, their non-compliance is excused.

277. PIA breached the Agreement by continuing to distribute, reproduce and/or publicly perform copies of Plaintiffs' Works in violation of U.S. Copyright law.

278. Plaintiffs relied upon the contract to their detriment for Defendant PIA to cease distributing, reproducing and/or publicly performing copies of Plaintiffs' Works in violation of U.S. Copyright law.

279. PIA breached the Agreement by failing to pay Plaintiffs the agreed upon

amount.

280. PIA's obligation to make the agreed upon payment was not excused or relieved.

281. PIA's breaches of the agreement were substantial failures to perform that are material.

282. Plaintiffs have suffered damages as result of PIA's breach of contract.

283. For example, PIA did not make the payment by 9/30/2021 despite Plaintiffs' counsel emphasizing the importance of this date.

284. For example, PIA has directly infringed many of Plaintiffs' Works multiple times since breaching the contract.

**VII. FIRST CLAIM FOR RELIEF
(Contributory Copyright Infringement based upon material contribution)**

285. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

286. Plaintiffs are the registered copyright owners of the Works, each of which contains an original work of authorship.

287. Defendant actively promotes its VPN service for piracy and encourages its customers ("end users") to use its VPN service for piracy.

288. Defendant's end users use the VPN service for piracy.

289. Defendant transmits, routes, or provides connections for transmitting copies of Plaintiffs' Works through a network under its control including servers provided by Sharktech in Denver, CO.

290. Defendant distributed at least a piece of the copyright protected Works to

others.

291. Defendant makes copies of said Works on said network when transmitting, routing, or providing connections for transmitting copies of Plaintiffs' Works through said network for its end users.

292. Defendant encourages end users to use the network to distribute and reproduce copies of Plaintiffs' Works.

293. Defendant encourages end users outside of the United States to access and use their servers and IP addresses in the United States to violate geographical restrictions of authorized platforms and publicly perform and/or distribute copies of the Plaintiffs' Works outside of the United States.

294. Plaintiffs did not authorize, permit, or provide consent to Defendant to copy, reproduce, distribute, publicly perform, or display their Works.

295. Defendant encourages end users outside of the United States to use the VPN service to access and use servers and IP addresses in the United States to publicly perform and/or distribute copies of the Plaintiffs' Works to the end users outside of the United States.

296. Defendant interferes with standard technical measures used by copyright holders to identify or protect copyright works by purposefully deleting the end users' log information. See 17 U.S.C. § 512(i)(1)(B).

297. Defendant knowingly supplies the services such as IP addresses and server access to the end users despite actual and/or constructive knowledge that its end users use the machinery to infringe Plaintiffs' exclusive rights.

298. Defendant and its paid affiliates promote the service for the purpose of infringing copyright protected Works including Plaintiffs.

299. Through its activities, Defendant knowingly and intentionally took steps that are substantially certain to result in direct infringements of Plaintiffs' Copyrighted Works, and that have resulted in such direct infringements in violation of Plaintiffs' copyrights.

300. Defendant's host providers such as Sharktech, Choopa, and M247 sent it thousands of Notices providing it with specific knowledge of the end users' ongoing infringements of Plaintiffs' Works.

301. Despite Defendant's knowledge that its end users were using its service to engage in widescale copyright infringements, Defendant failed to take simple measures or any reasonable steps to minimize the infringing capabilities of their service.

302. Despite having the ability to do so, Defendant refuses to even null-route the IP addresses of the end users where specific infringing activity has been identified and informed.

303. Despite having the ability to do so, Defendant refuses to save logs of the IP addresses of the end users where specific infringing activity has been identified and informed.

304. Despite having the ability to do so, Defendant refuses to block notorious piracy websites such as The Pirate Bay, YTS, RARBG and 1337 that the end use to infringe Plaintiffs' Works as promoted by Defendant.

305. Defendant is liable as a contributory copyright infringer for the infringing acts of the end users. Defendant has actual and constructive knowledge of the infringing

activity of the end users. Defendant knowingly caused and otherwise materially contributed to the unauthorized distributions of Plaintiffs' Works.

306. Defendant's infringements were committed "willfully" within the meaning of 17 U.S.C. § 504(c)(2).

307. By engaging in the contributory infringement alleged in this Fourth Amended Complaint, Defendant deprived not only the producers of the Works from income that could have been derived when the respective film was shown in public theaters and offered for sale or rental, but also all persons involved in the production and marketing of this film, numerous owners of local theaters and retail outlets and their employees, and, ultimately, the local economy. Defendant's misconduct therefore offends public policy

VIII. SECOND CLAIM FOR RELIEF (Vicarious Infringement)

308. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

309. Defendant is vicariously liable for the infringing acts of the end users' infringements including but not limited to its end users' direct infringements of Plaintiffs' exclusive right to distribute and reproduce copies of their Works.

310. Defendant has the right and ability to supervise and control the infringing activities that occur through the use of its service, and at all relevant times has derived a direct financial benefit from the infringement of Plaintiffs' copyrights.

311. Defendant has refused to take any meaningful action to prevent the widespread infringement by the end users despite having actual knowledge. Indeed, the ability of end users to use Defendant's service to distribute copies of Plaintiffs' Works with

knowledge that all log records of their activities will be deleted acts as a powerful draw for users of Defendant's service.

312. Defendant's end users are also motivated to become end users of Defendant due to their knowledge that they can use piracy apps such as Popcorn Time and ShowBox to pirate Plaintiffs' Works without any consequence because of Defendant's policy of ignoring notices of infringement and deleting logs.

313. Defendant's end users are also motivated to become end users of Defendant due to their knowledge that they can use Defendant's service to access legal platforms such as Netflix from unauthorized regions and stream or distribute Plaintiffs' Works to these unauthorized regions.

314. Defendant is therefore vicariously liable for the unauthorized distribution of Plaintiffs' Works.

**IX. THIRD CLAIM FOR RELIEF
(Contributory Copyright Infringement based upon intentional inducement)**

315. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

316. Defendant intentionally induced the infringement of Plaintiffs' exclusive rights under the Copyright Act, including infringement of Plaintiffs' exclusive rights to reproduce, publicly perform, and distribute copies of their Works.

317. As instructed and encouraged by Defendant, its end users purchase and install the VPN service to conceal their identities while engaging in movie piracy.

318. As instructed and encouraged by Defendant, its end users install piracy applications such as Popcorn Time to use on their devices while assigned IP addresses

by the Defendant's VPN services to conceal their identities while pirating Plaintiffs' Works.

319. As instructed and encouraged by Defendant, end users access servers in the United States from locations outside of the United States that are not authorized by legal platforms to stream, distribute or reproduce Plaintiffs' Works and stream, distribute or reproduce Plaintiffs' Works.

320. As instructed and encouraged by Defendant, end users access servers in the United States from locations outside of the United States to use BitTorrent to export copies of Plaintiffs' Works to locations outside of the United States in violation of Plaintiffs' exclusive rights to distribute their Works.

321. Defendant's end users use piracy applications to connect to sources that publicly perform and/or distribute copies of Plaintiffs' Works while anonymously connected to the Internet by Defendant's VPN services.

322. Defendant's end users connect to notorious piracy websites such as YTS to download torrent files to reproduce and distribute copies of Plaintiffs' Works while anonymously connected to the Internet by Defendant's VPN service exactly as promoted and encouraged to do by Defendant.

323. Defendant induces direct infringements of Plaintiffs' Works by encouraging the end users to use movie piracy applications such as Popcorn Time and ShowBox and to access websites such as YTS that facilitate, enable, and create direct links between its customers and infringing sources, and by actively inducing, encouraging, and promoting its VPN services as a means to "safely" use movie piracy applications for blatant copyright infringement by assuring customers that their identification information will be concealed.

324. Defendant induces direct infringements of Plaintiffs' Works by encouraging the end users to use the VPN service to access legal platforms such as Netflix to publicly perform or distribute copies of Plaintiffs' Works to unauthorized regions.

325. Defendant's intentional inducement of the infringement of Plaintiffs' rights in their Copyrighted Works constitutes a separate and distinct act of infringement.

**X. FOURTH CLAIM FOR RELIEF
(Secondary Liability for DMCA Violations)**

326. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

327. Defendant encourages the end users to access torrent files for copying copyright protected Works from notorious movie piracy websites such as The Pirate Bay, Torrentgalaxy, 1337x, RARBG and YTS.

328. Defendant's end users registered for accounts with piracy websites such as YTS and RARBG.

329. Defendant's end users knowingly and with the intent to induce, enable, facilitate, or conceal infringement of the Plaintiffs' copyright protected Works, distributed copyright management information ("CMI") that included false wording such as "TGx", "RARBG", "FGT" and "YTS" in violation of 17 U.S.C. § 1202(a)(2).

330. Defendant's end users, without the authority of Plaintiffs, or the law, distributed removed or altered CMI knowing that the CMI had been removed or altered to include the wording "TGx", "RARBG", "FGT" or "YTS" without the authority of Plaintiffs and knowing, or having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement of Plaintiffs' copyright protected Works in violation of 17 U.S.C. §

1202(b)(2).

331. Defendant's end users, without the authority of Plaintiffs, or the law, distributed Plaintiffs' Copyright protected Works knowing that the CMI had been removed or altered to include the wording "TGx", "RARBG", "FGT" or "YTS", and knowing, or having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement of the copyright protected Works in violation of 17 U.S.C. § 1202(b)(3).

332. Particularly, Defendant's end users knew that the CMI in the file names of the pieces had been altered to include the wording "TGx", "RARBG", "FGT" or "YTS".

333. Particularly, Defendant's end users distributed the file names that included CMI that had been altered to include the wording "TGx", "RARBG", "FGT" or "YTS".

334. Defendant's end users knew that the wording "TGx", "RARBG", "FGT" or "YTS" originated from notorious movie piracy websites which Defendant itself promoted to them and to which the end users have registered accounts.

335. Defendant's end users' acts constitute violations under the Digital Millennium Copyright Act, 17 U.S.C. § 1202.

336. Defendant is secondarily liable for the DMCA violations of its end users.

337. Defendant has actual and constructive knowledge of the end users' DMCA violations.

338. Defendant knowingly caused and otherwise materially contributed to these DMCA violations.

339. Defendant is vicariously liable for the DMCA violations of the end users.

340. Defendant has the right and ability to supervise and control the DMCA

violations that occur through the use of the service, and at all relevant times has derived a direct financial benefit from the DMCA violations complained of herein. Defendant has refused to take any meaningful action to prevent the widespread DMCA violations by its end users. Indeed, the ability of Defendant's end users to distribute torrent files from torrent websites such as YTS and the Pirate Bay that Defendant and its affiliates themselves promote and obtain file copies of the Works with altered CMI and distribute said copies while concealing their activities acts as a powerful draw for Defendant's end users. Defendant is therefore vicariously liable for the DMCA violations.

341. Plaintiff is entitled to an injunction to prevent Defendant from continuing to contribute to violations of 17 U.S.C. § 1202.

342. Plaintiff is entitled to recover from Defendant the actual damages suffered by Plaintiffs and any profits Defendant has obtained as a result of its wrongful acts that are not taken into account in computing the actual damages. Plaintiffs are currently unable to ascertain the full extent of the profits Defendant has realized by the violations of 17 U.S.C. § 1202.

343. Plaintiffs are entitled to elect to recover from Defendant statutory damages for its violations of 17 U.S.C. § 1202.

344. Plaintiffs are further entitled to costs and reasonable attorneys' fees.

XI. FIFTH CLAIM FOR RELIEF (Breach of Contract)

345. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

346. On or about Sept. 1, 2021, Plaintiffs, other rightsholders and Defendant PIA

entered into a settlement agreement (“Agreement”) to resolve the copyright claims and other claims.

347. The Agreement is a valid, binding and enforceable contract.

348. Plaintiffs substantially complied with their part of the contract.

349. Plaintiffs are excused from performance of their part of the contract that was not performed.

350. Plaintiffs relied upon this contract to their detriment.

351. PIA breached the Agreement by continuing to distribute, reproduce and/or publicly perform copies of Plaintiffs’ Works in violation of U.S. Copyright law.

352. PIA breached the Agreement by failing to pay Plaintiffs the agreed upon amount.

353. PIA’s obligation to make the agreed upon payment was not excused or relieved.

354. PIA’s obligation to not distribute, reproduce and/or publicly perform copies of Plaintiffs’ Works in violation of U.S. Copyright law was not excused or relieved.

355. PIA’s breaches of the Agreement were substantial failures to perform that are material.

356. Plaintiffs have been damaged as result of PIA’s breach of contract in an amount to be proven at trial and is entitled to injunctive relief to prevent any further breaches and damages.

357. Plaintiffs are also entitled to attorneys’ fees arising from PIA’s breach of contract and interest of 10 percent a year as provided in §478-2 of the Hawaii Revised

Statutes.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs respectfully request that this Court:

(A) enter permanent injunctions enjoining Defendant from infringing and contributing to infringements of the Plaintiffs' copyrighted Works and contributing to DMCA violations;

(B) enter permanent injunctions ordering Defendant to stop interfering with standard technical measures by deleting end user log information;

(C) order Defendant to adopt a policy that provides for the prompt suspension of end users for which it receives more than three unique notices of infringements of copyright protected Works and/or DMCA violations unless within 72 hours unless said end users makes a counter notification;

(D) order Defendant to adopt a policy of storing logs of end user access for at least two years to comply with the legal requirement not to interfere with standard technical measures used by copyright holders to identify or protect copyright works;

(E) order Defendant to block end users from accessing notorious piracy websites of foreign origin including those listed in the annual trade report of Notorious Foreign Markets published by the United States Government such as (a) YTS; (b) Piratebay; (c) Rarbg; (d) 1337x; and (e) PopcornTime on networks under their control to prevent further pirating of Plaintiffs' Works;

(F) enter an order pursuant to 17 U.S.C. §512(j) and/or 28 U.S.C §1651(a) that any service provider subject to US jurisdiction providing service for Defendant including

but not limited to Leaseweb, Choopa and Sharktech which Defendant uses to infringe Plaintiffs' Works immediately cease said service upon notice;

(G) award the Plaintiffs their actual damages from the copyright infringements and Defendant's profits in such amount as may be found; alternatively, at Plaintiffs' election, for statutory damages pursuant to 17 U.S.C. § 504(a) and (c);

(H) award the Plaintiffs actual damages from Defendant's contribution to DMCA violations and Defendant's profits in such amount as may be found; or, in the alternative, at Plaintiffs' election, for statutory damages per DMCA violation pursuant to 17 U.S.C. § 1203(c) for violations of 17 U.S.C. § 1202;

(I) award the Plaintiffs actual and punitive damages pursuant to Hawaii law for Defendant PIA's willful breach of the settlement agreement with malice aforethought;

(J) award the Plaintiffs their reasonable attorneys' fees and costs pursuant to 17 U.S.C. § 505 and/or 17 U.S.C. § 1203(b)(5);

(K) award the Plaintiffs their reasonable attorneys' fees and costs against Defendant PIA pursuant to Hawaii law for PIA's breach of the settlement agreement;

(L) grant the Plaintiffs any and all other and further relief that this Court deems just and proper.

The Plaintiffs hereby demand a trial by jury on all issues properly triable by jury.

DATED: Kailua-Kona, Hawaii, Oct. 25, 2022.

/s/ Kerry S. Culpepper
Kerry S. Culpepper
CULPEPPER IP, LLLC
75-170 Hualalai Road, Suite B204
Kailua-Kona, Hawaii 96740
Telephone: (808) 464-4047

Facsimile: (202) 204-5181
E-Mail: kculpepper@culpepperip.com
Attorney for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on the date below I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following e-mail addresses:

A. John Peter Mancini jmancini@mayerbrown.com,
4680105420@filings.docketbird.com, ajpmancini@aol.com,
jmarsala@mayerbrown.com

Paul Matthew Fakler pfakler@mayerbrown.com,
7018781420@filings.docketbird.com, jmarsala@mayerbrown.com

Daniel M. Rosales , Jr drosales@foxrothschild.com, drosales@mayerbrown.com,
rhanshe@foxrothschild.com

DATED: Kailua-Kona, Hawaii, October 25, 2022.

CULPEPPER IP, LLLC

/s/ Kerry S. Culpepper
Kerry S. Culpepper
Attorney for Plaintiffs