

PUBLIC VERSION

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO.: 11-CV-20427-WILLIAMS/TURNOFF

DISNEY ENTERPRISES, INC.,
TWENTIETH CENTURY FOX FILM
CORPORATION, UNIVERSAL CITY
STUDIOS PRODUCTIONS LLLP,
COLUMBIA PICTURES INDUSTRIES,
INC., and WARNER BROS.
ENTERTAINMENT INC.,

Plaintiffs,

v.

HOTFILE CORP., ANTON TITOV, and
DOES 1-10,

Defendants.

HOTFILE CORP.,

Counterclaimant,

v.

WARNER BROS. ENTERTAINMENT INC.,

Counter-Defendant.

**[REDACTED] MOTION AND MEMORANDUM OF LAW OF
DEFENDANT HOTFILE CORPORATION FOR PARTIAL
SUMMARY JUDGMENT BASED ON THE
THE DIGITAL MILLENNIUM COPYRIGHT ACT SAFE HARBOR**

TABLE OF CONTENTS

	Page
MOTION.....	1
MEMORANDUM OF LAW	1
I. INTRODUCTION	1
II. BACKGROUND ON HOTFILE AND THE UNDISPUTED FACTS RELEVANT TO THE DMCA SAFE HARBOR.....	3
A. Hotfile Is A Flexible Hosting Service That Works With Any Type of Digital File, Including Software Applications, Video And Many More	3
B. Hotfile Has Complied With the DMCA And Taken Proactive Measures to Combat Copyright Infringement Since Its Outset	6
C. Instead of Using DMCA Notices or the SRA Tool To Identify and Takedown Infringing Files, The Studios Filed This Action; Hotfile Responded By Continuing to Improve Its Policies and Technology	8
III. LEGAL STANDARD.....	10
A. Summary Judgment Standard	10
B. The Digital Millennium Copyright Act (“DMCA”)	10
IV. ARGUMENT: THE DMCA SAFE HARBOR FOR FILE HOSTING PROTECTS HOTFILE FROM THE STUDIOS’ CLAIMS AFTER FEBRUARY 18, 2011	12
A. Hotfile Did Not Have Knowledge Of The Files-In-Suit, And When It Received Notice Of the Claimed Infringing Links It Expeditiously Took Them Down	12
1. Hotfile Did Not Have Actual Or Apparent Knowledge of Any Of The Files-In-Suit.....	12
2. Whenever Hotfile Received Notice of The Claimed Infringements It Expeditiously Took Down Those Links.....	15
B. Hotfile Does Not Receive A Direct Financial Benefit Related to Infringement Nor Does It Have the Ability to Control the Alleged Infringing Activity	16
1. Hotfile Does Not Receive a Financial Benefit Directly Attributable to the Alleged Infringing Activity.....	16
2. Hotfile Does Not Have The Ability to Control The Alleged Infringement.....	17
C. Hotfile Has At All Times Maintained A Designated Agent To Receive DMCA Notifications And Registered An Agent With The Copyright Office	18

TABLE OF CONTENTS
(continued)

	Page
D. Hotfile Adopted And Reasonably Implemented An Appropriate Repeat Infringer Policy As Of February 18, 2011	19
V. CONCLUSION.....	21

MOTION

Pursuant to Rule 56 of the Federal Rules of Civil Procedure, Defendant Hotfile Corporation (“Hotfile”) hereby moves for summary judgment on the Studios’¹ copyright infringement claims from February 18, 2011 forward. There can be no genuine issue of material fact that during this time period Hotfile qualifies for the Digital Millennium Copyright Act (“DMCA”) safe harbor protection. Hotfile is accordingly entitled to judgment as a matter of law.² The motion is based on the attached declarations of Anton Titov and Deepak Gupta, the accompanying memorandum of law, the Statement of Material Facts and such other matter as may be presented.

MEMORANDUM OF LAW**I. INTRODUCTION**

Hotfile is a leader in Internet file-hosting and cloud storage. It has hosted over 100 million digital files for businesses and people around the world on its network and server infrastructure. These files include software, video, audio and virtually every other type of digital file that someone would want to store or share.

The DMCA established safe harbors to shield certain “common activities of [Internet] service providers” such as Hotfile that are integral to the Internet’s infrastructure (Dec. of Deepak Gupta (attached hereto as Exhibit A), Ex. 1 (S. Rep. No. 105-190 (1998), at 19).) 17 U.S.C. § 512(c) provides a safe harbor for file-hosting and related activities of the type provided by Hotfile. Congress enacted the DMCA “to foster *cooperation* among copyright holders and service providers in dealing with infringement on the Internet.” *UMG Recordings Inc. et al. v. Shelter Capital Partners LLC et al. and Veoh Networks, Inc.* -- F.3d --, 2011 WL 6357788, *10 (9th Cir. Dec. 20, 2011) (“*UMG Cir.*”) (citing S. Rep. No. 105-190, at 20). From its beginning in 2009,

¹ The Plaintiffs are five major motion picture studios: Disney Enterprises, Inc., Twentieth Century Fox Film Corporation, Universal City Studios Productions LLLP, Columbia Pictures Industries, Inc. and Warner Bros. Entertainment Inc. (collectively “Plaintiffs” or the “Studios”).

² Hotfile contends that the Studios will not be able to prove copyright liability for the pre-Complaint period and Hotfile should be entitled to DMCA safe harbor protection against copyright damages liability for its entire existence. As there may be genuine disputes about some facts before February 18, 2011, however, Hotfile does not seek summary judgment covering its activities before that date. It will establish its entitlement to protection for the earlier period, if necessary, at trial.

Hotfile has proactively cooperated with the Plaintiff Studios and other copyright owners to deter copyright infringement on its site. Hotfile has continually improved its copyright enforcement practices and procedures, by adopting new technologies and providing content owners with increasingly sophisticated tools to facilitate the rapid takedown of suspected infringing works, which is the bedrock of the DMCA.

General awareness of possible infringement on a network does not disqualify a service provider from the safe harbor. Under the DMCA, only actual or “red flag” knowledge of specific allegedly infringing files and a failure to expeditiously takedown those files, can result in liability. Indeed, service providers are not required to “affirmatively seek[] facts indicating infringing activity.” 17 U.S.C. § 512(m)(1). Rather, “[t]he DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright” *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007); *UMG Recordings*, at *11.

The Studios do not allege that Hotfile failed to takedown even a single reported URL or link. Instead, their theory of liability is that Hotfile should be liable for particular infringements of which it was *unaware*—unaware in many cases because the Studios elected not to report them. Case after case has rejected this argument. Such an exception to the safe harbor protection would return copyright law to a pre-DMCA age when internet service providers such as Hotfile faced the impossible task of policing tens of millions of files or risk potentially ruinous copyright liability.

Hotfile has embraced the DMCA, and at all times since its 2009 launch sought to comply with its obligations under the statute. There can be no genuine dispute that at least since its revamped repeat infringer policy was instituted in February 2011 Hotfile has strictly complied with all DMCA requirements and is entitled to safe harbor protection as a matter of law.³

³ As shown below, there can be no genuine dispute that (1) Hotfile has been a service provider under the DMCA, (2) Hotfile has maintained a registered DMCA agent with the Copyright Office, (3) Hotfile did not have actual or “red flag” knowledge of the files-in-suit, (4) whenever it received a DMCA-complaint notice of claimed infringement it expeditiously took down the noticed files, (5) Hotfile did not receive a direct financial benefit from the alleged infringing activity, (6) Hotfile did not have the practical ability to control the alleged infringements, (7) Hotfile accommodates and does not interfere with “any standard technical measures” used to protect content; and (8) that Hotfile, on February 18, 2011, adopted and reasonably implemented a DMCA-complaint “three-strikes” policy for terminating repeat infringers.

II. BACKGROUND ON HOTFILE AND THE UNDISPUTED FACTS RELEVANT TO THE DMCA SAFE HARBOR

A. Hotfile Is A Flexible Hosting Service That Works With Any Type of Digital File, Including Software Applications, Video And Many More.

Since its launch in 2009, Hotfile has offered premium file-hosting that enables its global user base to reliably store, use and share digital files. It works with literally any type of computer file. Hotfile is particularly well-suited to host large file types that are the future of the Internet. (Dec. of Anton Titov (attached hereto as Exhibit B), ¶ 2.)

When a person first signs up with Hotfile or uploads a file they must agree to Terms of Service and the Hotfile Intellectual Property Policy which prohibit copyright infringement. Upon uploading, they receive a private URL link that is known only to them. Users can keep these links private for their own “personal cloud storage.” Hotfile’s Privacy Policy assures its customers that they can feel comfortable storing personal material in this way. Registered users can store files for three months. If they want perpetual storage they must then upgrade to a premium account. (*Id.* ¶ 3; Ex. 3 at ¶¶ 21-24; Ex. 4 at 166:24-167:25; 178:23-179:25; 209:1-13 to Exhibit A.)⁴

Hotfile may also be used as an efficient method of sharing files that may be too large to be sent via email. Users may wish to give access to their files to co-workers, friends and family. They could, for example, share work documents with colleagues, or transfer weekend photos to family, or upload an HD video of their softball game and share it with members of their team. This is effectively a more advanced and convenient form of “FTP” or “File Transfer Protocol” which has existed on the Internet for decades. Similarly, Hotfile can be used to “space-shift” content so that a user can access their own documents on different devices in different places. (Exhibit B ¶ 4; Ex. 3 at ¶¶ 25-26 to Exhibit A; Ex. 4 at 109:9-111:13 to Exhibit A.)

Hotfile, like other Internet hosting services, promotes the widespread creation and sharing of user-generated content. With ubiquitous home recording studios powered by software like GarageBand™ and easy access to HD cameras and video-editing software like iMovie™, the abundance of creative digital works (and the corresponding larger files) being produced today is

⁴ Hotfile submits with this Motion the Rule 26 expert reports prepared by Professor James Boyle of Duke University in support of Hotfile along with authenticating testimony from his deposition. *See* Exhibits 2 and 3 to the Gupta Declaration (attached hereto as Exhibit A). Hotfile intends to submit a declaration from Prof. Boyle in connection with its Opposition to Plaintiffs’ Summary Judgment Motion.

growing and unprecedented. *See, e.g., UMG Cir.*, 2011 WL 6357788, *10 (“many music videos [] could in fact legally appear on Veoh,” including user generated content and major label content); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1136 (N.D. Cal. 2008) (Veoh “enables the sharing of user-provided video content over the Internet—from job interviews, to family gatherings, to films by aspiring filmmakers.”); *Wolk v. Kodak Imaging Network et al.*, 2012 WL 11270, *2 (S.D.N.Y.) (“The images and videos posted to Photobucket, of which there are approximately 9 billion, are generated by the users themselves.”); *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008) (video of child dancing to Prince song viewed over half a million times); *Viacom Int’l v. You Tube, Inc.*, 718 F. Supp. 2d 514, 518 (S.D.N.Y. 2010)(24 hours of video uploaded each minute).

Even traditional studios and labels share their works on the Internet to obtain free marketing. *UMG Recordings, Inc., v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099, 1110 n.13 (C.D. Cal 2009) (“*UMG Dist.*”) (artist affiliated with the plaintiff uploaded video to Veoh); *Capitol Records v. MP3 Tunes*, 2011 WL 5104616, *13 (S.D.N.Y. 2011) (“[A]s part of its innovative marketing, EMI itself regularly distributes works on the internet for free.”) This cultural shift toward user-generated content and authorized file-sharing heralds a sea change in the way content is created and consumed.

Hotfile is at the forefront of this trend. It hosts a wide variety and quantity of non-infringing digital content. As a provider of storage hosting services, Hotfile does not in the ordinary course of business review the files it stores, nor could it practically do so given that in its three-year existence more than 100 million files have been uploaded to its servers. However, through occasional communications with its users, Hotfile learned that various video files, music files, software programs and graphical content on Hotfile.com were uploaded by or with authorization of the content owner. (Exhibit B ¶ 5 (collecting examples).) Discovery has further confirmed that Hotfile hosts a variety of open source software packages, freely shared videos, Creative Commons movies and public domain books. (Ex. 2 at ¶¶ 13-23 (open source software), ¶¶ 24-28 (full length animated videos under Creative Commons licenses), ¶¶ 30-33 (Twain, Shakespeare and Dickens) to Exhibit A); Ex. 3 at ¶¶ 43 (redistributable software), ¶ 49 (book on Russian Fabric Patterns from 1871) to Exhibit A; Ex. 4 at 38:18-39:5 (authenticating opening expert report), 157:25-158:5 (Huck Finn), 44:3-45:15 (examples of freely distributable content) to Exhibit A; Ex. 5 at 257:14-258:6 (redistributable software) to Exhibit A.) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

While Hotfile, like any other service provider, can never eliminate all copyright infringements on its site, its proactive efforts have been demonstrably successful. Recently, Hotfile implemented vCloud9, the video fingerprinting product touted as capable of identifying copyrighted content on a cloud storage service, which Plaintiffs' trade association, the Motion Picture Association of America states "ensure[s] copyright compliance." (HF Facts 26-27.) vCloud9 software has identified *less than 5% of audio/video files* uploaded to Hotfile as "matches" for content in Vobile's database, which includes the copyrighted content of each of the Studios and many other content owners. Hotfile, of course, blocks these. (*Id.*; Exhibit B ¶ 35 and Ex. 38.)

Hotfile has a "freemium" business model. Users can store files for a limited time and get downloads at limited speeds for free. Hotfile's revenues come solely from users who upgrade to "premium" subscriptions. Premium users pay up to \$9 per month for faster downloads, permanent file storage, and other benefits. This fixed fee does not vary based on what or how much users are consuming—they could be using Hotfile for personal cloud storage, downloading open source software, or streaming video. The fee compensates Hotfile for its substantial investments in building out its state-of-the-art data network and server infrastructure. Hotfile has no advertising and derives no advertising revenue. (Exhibit B ¶ 7.)

As do many other web based business, such as Amazon.com, Hotfile offers an "affiliate program" that distributes a portion of its revenue to users whose actions generate more premium subscribers. Hotfile's affiliate program applies equally to all forms of digital files, regardless of whether they are video, software or anything else. Hotfile's affiliate program allows the authors of copyrighted works to upload their content and be paid for its distribution on the Internet. The files most frequently downloaded from Hotfile are non-infringing software files uploaded as part of the affiliate program. (Exhibit B ¶ 8.) The affiliate program, thus, provides a novel and important way to compensate content creators, including the growing user-generated community, for the "free" distribution of their works on the Internet. (Ex. 2 at ¶¶ 20-21, 37 to Exhibit A; Ex. 4 at 52:1-53:4, 149:6-151:8 to Exhibit A; Ex. 5 at [REDACTED] to Exhibit A.)

In sum, Hotfile is carrying out precisely the type of activities that Congress sought to encourage with the passage of the DMCA – it is expanding the “speed” and “capacity” of the Internet and, in doing so, it is expanding the “variety” and “quality” of services on the Internet. (Ex. 1 to Exhibit A (S. Rep. No. 105-190, at 8).)

B. Hotfile Has Complied With the DMCA And Taken Proactive Measures to Combat Copyright infringement Since Its Outset.

The DMCA, “preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment.” (Ex. 1 to Exhibit A (S. Rep. No. 105-190, at 20).) The bedrock of that cooperation is the DMCA’s allocation of the burden of identifying infringing links on content owners and the corresponding obligation that it places on service providers of taking down those links. Hotfile has embraced this cooperative approach since day one.

Hotfile’s firm stance against copyright infringement is well documented. Its original February 2009 Terms of Service expressly stated, “Transmission, distribution, or storage of any materials that violate laws is forbidden. This includes without restriction ... *copyright laws* ... and other intellectual property rights.” Hotfile also expressly “reserve[d] the right to immediately suspend or delete the account of a client, which, in the opinion of Hotfile, offends the present agreement or laws or decisions [including] offend[ing] copyrights...” (Exhibit B ¶ 12 and Ex. 8.) The first version of Hotfile’s website included a “report abuse” form in which content owners would input an allegedly infringing URL. This instantly generated a message to Hotfile’s abuse department. In response, Hotfile expeditiously took down the link. (*Id.*, ¶ 13 and Ex. 9.) Hotfile has continuously made the abuse@hotfile.com email address available on its website. Content owners, including the Studios and their agents, have consistently utilized Hotfile’s notice-and-takedown processes and Hotfile has expeditiously responded to takedown notices. (*Id.* ¶¶ 13-14)

In April 2009, within months of its launch, Hotfile posted a policy that expressly referenced the DMCA. (Exhibit B ¶ 15 and Ex. 15.) Also in April 2009, Plaintiff Warner Brothers suggested to Hotfile that having a “takedown tool” to more quickly remove infringing content “rather than sending an official takedown abuse notice every time URL’s are identified” would be “ideal.” (Exhibit B ¶ 20 and Ex. 21; Ex. 8 at 17:2-18:6, 18:19-24, 19:8-9 to Exhibit A.) Based on this idea, Hotfile engineered and offered “SRAs” (special rightsholder accounts) to streamline notice-and-takedowns for sophisticated content owners such as Warner. With SRAs, rightsholders who attest under the DMCA that they have authority of the copyright owner can enter URLs for files on

Hotfile's systems, and those files are automatically taken down; no further action by Hotfile is required. (Exhibit B ¶ 21.) HBO approved the philosophy behind SRAs, acknowledging that "a faster way to remove [] infringing links is required in solving [the] problem." (Ex. 32 to Exhibit B.)

SRAs became available in the summer of 2009. Hotfile notified the Studios and other content owners of the availability of the SRAs. (HF Fact 9.) Many content owners, including these Studios, and their content-protection agents have used Hotfile SRAs extensively and effectively. Today, there are approximately one hundred SRAs in active use. (HF Fact 10.) The Studios have professed satisfaction with this technology as a way to protect their content. They have thanked Hotfile for its "fast cooperation," and its "commitment to copyright compliance." (HF Fact 11.) Plaintiff Warner requested another hosting site, Fileserve.com, to implement "[a]n automated way to remove files," similar to Hotfile's SRA. (HF Fact 12.)

Soon after making SRAs available, Hotfile implemented hashing technology so that once a file was deleted (by SRA or DMCA takedown notice) all identical copies were removed from the system and the same file was prevented from being uploaded again by the same user or others, even under a different name. This was accomplished with an MD5 hash which is "almost like a fingerprint" for each file. (HF Fact 13.)

In December 2009, Hotfile formally registered a Designated DMCA Agent with the U.S. Copyright Office, who could be contacted by content owners for takedown requests. (HF Fact 3.) The abuse@hotfile.com email address continued to be available as well. In approximately May 2010, Hotfile updated the Intellectual Property policy on its website to include the name and address of its Designated Agent and notification of its repeat infringer termination policy. That information has remained in place continuously since that time. (HF Facts 4-5.)

Since its outset, Hotfile has exercised its discretion to terminate users for repeat copyright infringement. Its records show more than forty account terminations for repeat copyright infringement before the filing of this action in February, 2011. (Ex. 35 to Exhibit B, HF00000048.) In addition, there were many similar terminations carried out early on before such records began to be retained in the Hotfile database. (Exhibit B ¶ 31; Ex. 9 to Exhibit A.)

Hotfile and Plaintiff Warner also discussed cooperation on a commercial level. In 2010, Warner proposed a business partnership to use Hotfile as a distribution platform by including links on Hotfile to ecommerce sites where Warner Bros content is hosted. (Exhibit B ¶ 28) As part of

those discussions, Warner suggested that links from Hotfile would go to “iTunes, Amazon [and] WBSshop” so that Hotfile could obtain “affiliate commissions.” (Exhibit B ¶ 28 and Ex. 34; Ex. 10 at 186:25-191:25 (authenticating exhibit) to Exhibit A.)

With its prompt takedown procedures, SRAs, and fingerprinting, and in light of the Studios’ uniform praise and lack of requests for additional countermeasures beyond SRAs, until learning of the filing of this Complaint, Hotfile reasonably believed that its cooperation with the content owners, including Plaintiffs, was successful. It had no reason to believe that its content protection policies were not satisfactory to the Studios. The filing of this lawsuit on February 8, 2011 without warning thus came as a rude surprise. (Exhibit B ¶ 29.)

C. Instead of Using DMCA Notices or the SRA Tool To Identify and Takedown Infringing Files, The Studios Filed This Action; Hotfile Responded By Continuing to Improve Its Policies and Technology.

When the Studios filed their Complaint, they attached a list of 150 “representative works” but did not identify to Hotfile—in the Complaint or otherwise—a single URL (or link) to any allegedly infringing file. (Complaint, Dkt. 1.) As a result, Hotfile had no way to identify the allegedly infringing files. Only after several months of discovery, and repeated requests from Hotfile’s counsel, did Plaintiffs identify an initial list URLs in an interrogatory answer. (Ex. 11 to Exhibit A.) Then, after first gaining access to Hotfile’s entire database, Plaintiffs in the end produced a list of approximately 900,000 files on Hotfile (less than 1% of the files ever hosted on Hotfile) that they now contend infringe their copyrights. Plaintiffs’ Counsel stated they spent “hundreds of man-hours, maybe thousands,” to generate this list—yet the list contained numerous errors. (Ex. 10 at 89:2-13 to Exhibit A.)

Upon reviewing the Complaint, Hotfile learned for the first time – after years of professed satisfaction with Hotfile -- that the Studios were not satisfied with its repeat infringer policy. (Complaint ¶ 42.) Within weeks of the filing of the complaint on February 18, 2011, Hotfile proactively instituted a “three-strikes” policy similar to those which have been recently upheld as a matter of law in several cases. (HF Fact 21.) Under this policy, Hotfile tracks how many times it receives notices of claimed infringement for files uploaded by a particular user. Once a user receives three qualifying notices their account is permanently terminated, all of the files they uploaded are deleted and their email address is blacklisted. (HF Fact 22.) Since February 18, 2011, Hotfile has terminated thousands of users pursuant to this strengthened repeat infringer policy. (Exhibit B ¶33 and Ex. 35.)

In the summer of 2011, Hotfile supplemented its hash fingerprinting technology by adopting Vobile MediaWise. This technology identifies files that have characteristics matching content registered by copyright owners, including each of the Plaintiffs, in Vobile's database which Hotfile then blocks. (HF Fact 25.) It can identify files that have never been subject to a takedown notice and goes beyond DMCA requirements.

In September 2011, Vobile acknowledged that MediaWise was incompatible with storage sites like Hotfile, and launched "VCloud9," which it claims is effective for cloud storage sites like Hotfile. Hotfile is now using this state of the art package, which the MPAA states "ensures copyright compliance." Using vCloud9, Hotfile blocks the 4-5% of audio/video content on Hotfile that vCloud9 identifies as infringing. (HF Fact 26; Exhibit B ¶ 35 and Ex. 38.)

In its continuing efforts to improve its policies to combat copyright infringement, Hotfile recently modified its Affiliate Program. It no longer counts password protected files for potential affiliate credit, no longer offers a site referral affiliate program, and counts credits only based on premium conversions (not download counts). It now suspends any affiliate who receives a strike from the program and requires them to attend an online "copyright school" to be reinstated. Another strike will result in expulsion from the affiliate program (and a third strike results in account termination). (HF Fact 28.)

These additional countermeasures go beyond what the Studios demanded in their Complaint or ever requested in this litigation. Hotfile will continue to improve and adjust its policies to ensure effective DMCA compliance and will cooperate with willing content owners.

III. LEGAL STANDARD

A. Summary Judgment Standard

"The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). *Accord Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Once a party demonstrates the absence of a genuine issue of material fact, the nonmoving party must "go beyond the pleadings and by her own affidavits, or by the 'depositions, answers to interrogatories, and admissions on file,' designate 'specific facts showing that there is a genuine issue for trial.'" *Id.* at 324. "Where the record taken as a whole could not lead a rational trier of fact to find for the nonmoving party, there is no 'genuine issue for trial,'" and summary judgment is appropriate. *See*

Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986) (quoting *First Nat'l Bank of Ariz. v. Cities Serv. Co.*, 391 U.S. 253, 289 (1968)).

B. The Digital Millennium Copyright Act (“DMCA”)

The DMCA safe harbors were intended “to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.” S. Rep. No. 105-190, at 1-2 (quoted in *Io*, 586 F. Supp. 2d at 1141). Recognizing that it “will not serve anyone’s interest if the Internet’s backbone and infrastructure are sued out of existence for involvement in purportedly aiding copyright infringement” (Nimmer on Copyright § 12B.01[C][1]), Congress enacted the safe harbors to protect internet service providers from, among other things, liability “for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network....” 17 U.S.C. § 512(c)(1).⁵

Hosting providers who satisfy the conditions of the statute have a safe harbor from “*all monetary relief* for direct, vicarious and contributory infringement. (S. Rep. 105-190, at 40 (emphasis added)(Ex. 1 to Exhibit A.); 17 U.S.C. § 512(c). They can only be subject to a limited injunction. 17 U.S.C. § 512(j).⁶ Here are the straightforward safe harbor requirements:

[A] No knowledge (actual or red-flag) / Expeditious takedown. The service provider must (i) not have actual or “red-flag” knowledge (based on awareness of “facts or circumstances from which infringing activity is apparent”) of the specific files alleged to be infringing, (17 U.S.C. § 512(c)(1)(A)(i) & (ii)); or (ii) if the service provider obtained actual or “red flag” knowledge of the specific files alleged to be infringing, either through a DMCA-compliant takedown notice or independently, it must have expeditiously disabled those files. (17 U.S.C. § 512(c)(1)(A)(iii) & (c)(1)(C));

[B] No direct financial benefit where right and ability to control infringement. The service provider must (i) not have received a financial benefit directly attributable to the infringing activity, (ii) where the service provider had the right and practical ability to control the activity. (17 U.S.C. § 512(c)(1)(B));

⁵ The alleged infringement relates to “storage at the direction of users” and is accordingly eligible for the 17 U.S.C. § 512(c) safe harbor. The Studios’ claim for “direct infringement” was dismissed because “nothing in the complaint alleges that Hotfile or Mr. Titov took direct, volitional steps...” to infringe. (Docket 94 (Order on Motion Dismiss at 4, 7.)) Thus, only the “indirect infringement” claim remains, and this fundamentally alleges that *users* are uploading infringing files. See *UMG Cir.*, 2011 WL 6357788, at * 9 (where Veoh “established a system whereby software automatically processes user-submitted content” and processes were “initiated entirely at the volition of Veoh’s users,” threshold satisfied).

⁶ The pertinent portions of 17 U.S.C. § 512 for the “storage at the direction of a user” safe harbor being claimed by Hotfile are attached hereto as Appendix A.

[C] Designated agent. The service provider must designate an agent to receive DMCA takedown notices on its website and with the Copyright Office. (17 U.S.C. § 512(c)(2));

[D] Repeat infringer policy. The service provider must adopt, reasonably implement and inform subscribers of a policy for terminating repeat infringers that is appropriate under the circumstances. (17 U.S.C. § 512(i)(1)(A)); **and**

[E] Not interfere with standard technical measures. The service provider must accommodate and not interfere with standard technical measures. (17 U.S.C. § 512(i)(1)(B)).

The DMCA's plain allocation of responsibilities and demarcation of safe harbors encourages service providers like Hotfile to "make the necessary investment in the expansion of the speed and capacity of the Internet....[B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand." (S. Rep. No. 105-190, at 8, Ex. 1 to Exhibit A.)

Where as here the facts establishing that the service provider⁷ has met these requirements are not in genuine dispute, courts have not hesitated to grant summary judgment:

- *UMG Recordings Inc. et al. v. Shelter Capital Partners LLC et al. and Veoh Networks, Inc.*, 2011 WL 6357788 (9th Cir. 2011) ("UMG Cir.") affirmed safe harbor for video hosting site Veoh, and found Veoh not liable for infringements by users of which it was unaware. *See, also, Io*, 586 F. Supp. 2d 1132 (C.D. Cal. 2009) and *UMG Recordings, Inc v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009) ("UMG Dist.") (trial court's granting summary judgment of safe harbor for Veoh).
- *Capitol Records, Inc. v. MP3Tunes, LLC*, 2011 WL 5104616 (S.D.N.Y.), safe-harbored a cyberlocker that allowed users to upload files from their hard-drive and "side-load" files from all over the Internet for storage and streaming. The service could be liable only for files that users had side-loaded from URLs that the Plaintiff had specifically identified to the cyberlocker by URLs in a DMCA compliant takedown notice, which the service failed to take down.
- *Wolk v. Kodak Imaging Network, Inc.*, 2012 WL 11270 (S.D.N.Y. 2012) safe-harbored photo-sharing Internet Service provider Photobucket.com against claims that users of Photobucket were copying, displaying and modifying copyrighted artwork, even despite allegations that "Photobucket's search function can, in some categories, cause a user to have search results with more than 70% of the images displayed being protected by copyright." *Id.* at *5.
- In *Perfect 10, Inc. v. Google, Inc.*, No. CV 04-9484(AHM) (July 26, 2010, C.D. Cal.) the court granted partial summary judgment in favor of Google for its web and image search and Blogger services, where notices of infringement by the Plaintiff were inadequate. (*See* Ex. 12 to Exhibit A.)

⁷ "Plaintiffs do not and will not contend, for purposes of this litigation, that Hotfile is ineligible for the DMCA safe harbor at 17 U.S.C. § 512(c) by virtue of not being a 'service provider' under 17 U.S.C. § 512(k)(1)(B)." (HF Fact 1.)

- *Viacom Int'l v. You Tube, Inc.*, 718 F. Supp. 2d 514 at 527-28 (S.D.N.Y. 2010) granted safe harbor to YouTube. The facts that YouTube inserted for-profit advertising and generated searchable indexes of video to provide a complete video entertainment experience did not nullify the safe harbor.
- In *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1110-11 (W.D. Wash. 2004) the court granted safe harbor to a service enabling vendors to upload images onto Amazon's servers, which were then displayed to users.

Here, too, there is no genuine dispute that Hotfile satisfies the DMCA safe harbor requirements for the post-February 18, 2011 time period.

IV. ARGUMENT: THE DMCA SAFE HARBOR FOR FILE HOSTING PROTECTS HOTFILE FROM THE STUDIOS' CLAIMS AFTER FEBRUARY 18, 2011.

A. Hotfile Did Not Have Knowledge Of The Files-In-Suit, And When It Received Notice Of the Claimed Infringing Links It Expeditiously Took Them Down.

1. Hotfile Did Not Have Actual Or Apparent Knowledge of Any Of The Files-In-Suit.

The safe harbor applies to a service provider that does “not have actual knowledge that the material or an activity using the material on the system or network is infringing and [is] not aware of facts or circumstances from which infringing activity is apparent. Where a service provider does obtain either actual or apparent knowledge, it may still enjoy the ‘safe harbor’ if it acts expeditiously to remove or disable access to the infringing material.” *Wolk*, 2012 WL 11270, *20. Hotfile did not have knowledge of the specific files-in-suit prior to being notified by the Studios, and when it received notice of any it expeditiously took them down. Accordingly, it cannot be charged with disqualifying knowledge under the DMCA.

Case after case holds that to disqualify a service provider from DMCA safe harbor, it must have knowledge of the specific instances of alleged infringement and have failed to act:

Requiring specific knowledge of particular infringing activity makes good sense in the context of the DMCA, which Congress enacted to foster cooperation among copyright holders and service providers in dealing with infringement on the Internet. *See S.Rep. No. 105-190*, at 20 (noting OCILLA was intended to provide “strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements”); *H.R.Rep. No. 105-551, pt. 2*, at 49 (1998) (same). Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh, who cannot readily ascertain what material is copyrighted and what is not.

UMG Cir., 2011 WL 6357788, *10.

As with the test for actual knowledge, the “apparent knowledge” test – also known as the “red-flag” test – requires awareness of “facts or circumstances” related to **specific items**. In *UMG Recordings*, the Plaintiff (Universal Music Group) argued that hosting site “Veoh hosted a category of copyrightable content – music – for which it had no license from any major music company” and it had “general knowledge that its services could be used to post infringing material.” *UMG Cir.*, 2011 WL 6357788, **9-11. Indeed, it tagged many files as “music videos.” *Id.*, *12. Noting that “there are many music videos that *could* in fact legally appear on Veoh” the court ruled, “general knowledge that it hosted copyrightable material and that its services could be used for infringement is insufficient to constitute a red flag.” *Id.*, *11 (no “investigative duties” on service providers); *see also*, *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007). Disqualifying service providers from DMCA safe harbor based on anything less than knowledge of *specific instances* of infringement is at odds with the language of the statute, which presumes that the red flag “aware[ness] of facts or circumstances from which infringing activity is apparent” should enable the service provider to “expeditiously [] remove, or disable access to the material that is claimed to be infringing or to be the subject of infringing activity” for which safe harbor is sought. 17 U.S.C. § 512(c)(iii) (emph. added).

A critical mass of legal precedent is now in accordance that a service provider will be denied the protection of the safe harbor only if it knows of *specific instances* of the alleged infringement that it fails to take down. *See Viacom*, 718 F. Supp. 2d at 519, 525 (“if a service provider knows (from notice from the owner, or a ‘red flag’) of *specific instances* of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the infringement.” (emphasis added)); *Capitol Records*, 2011 WL 5104616, *13 (no red flag knowledge based on employee’s downloading of “popular” artists from sites like rapidshare.com, and content owners providing lists of “representative works,” without identifying infringing URLs; disqualification only as to those URLs of which the service provider had notice); *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 106-07 (2d Cir. 2010) (eBay’s “generalized” knowledge of counterfeit goods being sold on its website was insufficient for contributory trademark infringement liability where Ebay disabled listings when provided specific listing numbers); *Wolk*, 2012 WL 11270, *20 (rejecting a rule “where one notice of infringement would apply to all instances of the image appearing on the website...[This rule] could result in Photobucket unlawfully blocking others from uploading images to which they hold valid

licenses.”)

Hotfile did not have actual or apparent “red flag” knowledge of specific instances of infringement among the files that the Studios have accused of infringing. (HF Fact 14.)⁸ Hotfile does not in the ordinary course of business review the millions of files its users upload. Independent of copyright owner reports and the occasional report from a third-party, Hotfile does not come to know of specific files that are alleged to be infringing. (HF Fact 15.) Hotfile cannot independently review the 100 million+ files its users are hosting to separate the infringing files from the many types of non-infringing files it hosts; its focus is on tuning and optimizing its server and network infrastructure.⁹ (Exhibit B ¶ 6.) The accused files are “a small fraction [<1%] of works posted to” Hotfile. (HF Fact 16); *Capitol Records*, 2011 WL 5104616, *13. Indeed, Hotfile respects its user privacy; users can accordingly feel confident using Hotfile for personal cloud storage, space-shifting and transferring files to family, friends and colleagues, if they wish. (Exhibit B ¶¶ 2-4.)

Hotfile went beyond what many sites do by taking down not only files expressly subject to DMCA notifications, but also taking down files based on MD5 hashes and Vobile fingerprinting. (Facts 13, 25, 26, 27.) *See UMG Cir.*, 2011 WL 6357788, *22 (discussion of “hash filtering”); *Io*, 586 F. Supp. 2d at 1154 (“Veoh’s digital fingerprint technology also prevents the same infringing

⁸ The Studios made a conscious decision “to forgo the DMCA notice protocol [which] ‘stripped [them] of the most powerful evidence of a service provider’s knowledge – actual notice of infringement from the copyright holder,’” for these files. *UMG Cir.*, 2011 WL 6357788, *9, citing *Corbis Corp. v. Amazon.com, Inc.*, 351 F.Supp. 2d 1090, 1107 (W.D.Wash. 2004) (citing 3 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 12B.04(A)(3), at 12B-53 [hereinafter “Nimmer”]); *see also Io*, 586 F. Supp. 2d at 1148.

⁹ It took the Studios “hundreds of man-hours, maybe thousands,” to create their list of accused infringing files, many of which were incorrect. Similarly, it took the Studios’ purported copyright law expert 225-275 hours to conduct a survey of a mere 1750 files on Hotfile at a cost of \$45,000. He now states he needs more information to make determinations as to some of the files he concedes were “closer calls.” (Ex. 5 at (Day 1) 26:20-27:4, 152:21-153:4, and (Day 2) 238:2-238:18, 286:8-287:23 to Exhibit A.) Hotfile cannot be expected to perform comparably extensive investigations for all the files it hosts. To the contrary, Congress believed that service providers should not be required “to make discriminating judgments about potential copyright infringement.” (S. Rep. No.105-190, at 49, Ex. 1 to Exhibit A.) And the DMCA expressly imposes no duty on service providers to monitor the files that users upload to their systems. *See Wolk*, 2012 WL 11270, at *22 (Photobucket has 9 billion files and there is no duty to monitor); 17 U.S.C. § 512(m). Plaintiff Warner’s undisputedly incorrect identifications, which are the subject of Hotfile’s counterclaim, show the difficulties of monitoring.

content from ever being uploaded again. All of this indicates that Veoh has taken steps to reduce, not foster, the incidence of copyright infringement on its website.”); *Compare Capitol Records*, 2011 WL 5104616, *15 (DMCA safe harbor except for copies of noticed files site “failed to remove from user lockers”; Hotfile MD-5 removes all user copies.) Hotfile thus did not know of or turn a blind eye to infringing files.

2. Whenever Hotfile Received Notice of The Claimed Infringements It Expeditiously Took Down Those Links.

The core feature of the DMCA’s approach to content protection is that content owners must identify and report particular infringements and service providers must respond expeditiously by taking down the identified content. Here, the Complaint suggests the Studios are generally dissatisfied with notice-and-takedown regime of the DMCA, complaining that it makes them play “catch-up” (Complaint ¶ 37), but it does not allege that Hotfile failed to expeditiously take down any URL that was subject to a takedown notice. *See* Complaint ¶ 38 (no allegation of failure to expeditiously take down in response to DMCA notices). This was confirmed in discovery. The Studios have not identified a single allegedly infringing URL listed in a takedown notice to Hotfile that was not expeditiously taken down. (HF Fact 18.) They cannot, because Hotfile’s robust notice-and-takedown procedures and SRA blocked all noticed URLs within 48 hours. (HF Facts 8-11, 17.) *See UMG Cir.*, 2011 WL 6357788, *14 (no liability for red flag knowledge where, “UMG has not specifically alleged that Veoh failed to expeditiously remove the infringing content identified by the user’s email, or that the content at issue was owned by UMG.”); *Io*, 586 F. Supp. 2d at 1150 (granting summary judgment where evidence showed that, when service provider “receives DMCA-compliant notice of copyright infringement, it responds and removes noticed content as necessary on the same day the notice is received (or within a few days thereafter)”).

B. Hotfile Does Not Receive A Direct Financial Benefit Related to Infringement Nor Does It Have the Ability to Control the Alleged Infringing Activity.

In order to qualify for the Section 512(c) safe harbor Hotfile must [1] “not receive a financial benefit directly attributable to the infringing activity, [2] in a case in which [it] has the right and ability to control such activity.” 17 U.S.C. § 512(c)(1)(B). A service provider loses safe-harbor eligibility only if the plaintiff can show *both* that the service provider had the right and ability to control the alleged infringements *and* received a financial benefit directly attributable to those infringements. *Corbis*, 351 F. Supp. 2d at 1109. The Studios show neither.

1. Hotfile Does Not Receive a Financial Benefit Directly Attributable to the Alleged Infringing Activity.

Hotfile receives the same fixed fees from its premium users regardless of how the person uses Hotfile. Much like with familiar broadband services, such as Comcast, Hotfile is content-neutral -- the premium user pays fees to Hotfile for faster download speeds regardless of the contents of the files being downloaded. (Facts 20-21.) As set forth in the legislative history, this does not constitute a “direct financial benefit” attributable to the alleged infringing activity:

In general, a service provider conducting a legitimate business would not be considered to receive a “financial benefit directly attributable to the infringing activity” where the infringer makes the same kind of payment as non-infringing users of the provider’s service. Thus, receiving a one-time set-up fee and flat periodic payments for service from a person engaging in infringing activities would not constitute receiving a “financial benefit directly attributable to the infringing activity.”

(S. Rep. No. 105-190, at 44, Ex.1 to Exhibit A.) With Hotfile, “infringer[s] make[] the same kind of payment as non-infringing users of the provider’s service,” and that payment consists of “flat periodic payments.” *Id.*; *Capitol Records*, 2011 WL 5104616, *14 (infringing and non-infringing users “paid precisely the same or nothing at all”). Hotfile “did not promote infringement” to “enhance the sale of user accounts.” *Id.* Rather Hotfile “removed infringing links” and “terminated the accounts of users who blatantly shared copyrighted files with others.” *Id.*

The Studios must concede that “any link between infringing activity and a direct benefit” to Hotfile is particularly “attenuated” here, because Hotfile users convert to premium accounts in order to download the files that the Studios’ expert selected and contends are “non-infringing” at a rate *five times higher* than those files he “confirmed” are infringing. *Id.* (Exhibit B ¶ 11; Ex. 3 at p. 23 to Exhibit A; Ex. 4 at 444:4-16, 446:2-19 to Exhibit A (based on Studios’ own commissioned study, “Hotfile was gaining economic success from noninfringing material, number one, I can conclude that; and number two, that they were actually gaining more economic success proportionately from noninfringing material than from confirmed infringing or highly likely infringing material.”) Even if the Studios’ statistics were true (the study is fatally flawed), what they would show is that Hotfile gets a relatively smaller financial benefit from users posting allegedly infringing Studio content compared to non-infringing content.

2. Hotfile Does Not Have The Ability to Control The Alleged Infringement.

The DMCA’s control inquiry requires the *practical ability* to control the specific

infringement at issue, something Hotfile did not have. “[T]he ‘right and ability to control’ the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored on its system.” *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2009). Indeed, Congress *presupposed* that service providers would have control over their systems, as the safe harbor expressly applies to material “that resides on a system or network *controlled* or operated by or for the service provider.” § 512(c)(1) (emphasis added). *Hendrickson*, 165 F. Supp. 2d at 1093; *see also UMG Dist.*, 665 F. Supp. 2d at 1113-15; *Io*, 586 F. Supp. 2d at 1151-52; *Corbis*, 351 F. Supp. 2d at 1110.

Rather, the “right and ability to control” analysis requires “something more.” *Capitol Records*, 2011 WL 5104616, *14. It focuses on the service provider’s practical control and requires the service provider to have knowledge and awareness of the specific infringing files.

As discussed, in the knowledge context it is not enough for a service provider to know as a general matter that users are capable of posting unauthorized content; more specific knowledge is required. Similarly, a service provider may, as a general matter, have the legal right and necessary technology to remove infringing content, *but until it becomes aware of specific unauthorized material, it cannot exercise its “power or authority” over the specific infringing item. In practical terms, it does not have the kind of ability to control infringing activity the statute contemplates.*

UMG Cir., 2011 WL 6357788, *15 (emphasis added). *See also, Viacom*, 718 F. Supp. 2d at 527 (“The ‘right and ability to control’ the activity requires knowledge of it, which must be item-specific...the provider must know of the particular case before he can control it.”); *Wolk*, 2012 WL 11270, *21 (“such a right and ability to control must take the form of prescreening content, rendering extensive advice to users regarding content and editing user content”.)

Hotfile does not have knowledge of what its users upload and does not control this. *See pp.* 12-15, *supra*. It is the users who select files and Hotfile “does not participate in those decisions.” *Capitol Records*, 2011 WL 5104616, *14. Hotfile also did not “willfully bury its head in the sand.” *UMG Cir.*, 2011 WL 6357788, *16. To the contrary, it offered SRAs, adopted MD5 hash technology, which the Studios’ expert concedes is “almost a fingerprint,” and supplemented this with Vobile fingerprinting. (Facts 8-13, 25-27.) Hotfile could have done nothing more and was certainly not obligated to. 17 U.S.C. § 512(m)(1). The control inquiry does not require a service provider to “adopt specific filtering technology and perform regular searches” for potentially infringing material. *UMG Dist.*, 665 F. Supp. 2d at 1113. Indeed, the DMCA bars “condition[ing]

the applicability” of the safe harbors on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.” *See, also, Perfect 10*, 508 F.3d at 1174 (Google’s “supervisory power limited” because it could not “analyze every image on the [I]nternet, compare each image to all the other copyrighted images that exist in the world ... and determine whether a certain image on the web infringes someone’s copyright.”) Hotfile did all that was reasonably within its “ability” and “control” to assist content owners and cannot be charged with control over the allegedly infringing activity.

C. Hotfile Has At All Times Maintained A Designated Agent To Receive DMCA Notifications And Registered An Agent With The Copyright Office.

Hotfile has had a “designated [] agent to receive notifications of claimed infringement” (17 U.S.C. § 512(c)(2)) on its website since its launch in February 2009. Since the beginning, content owners could use a report abuse form made “available [] on [the Hotfile] website in a location accessible to the public” (17 U.S.C. § 512(c)(2)) to reach its abuse department at the abuse@hotfile.com email address. (HF Facts 3-4.) Hotfile registered its designated agent with the Copyright Office in December 2009, and posted its agent’s name and address to the site by May 2010. (HF Fact 4.) Content owners – including the Studios -- have had no difficulty contacting Hotfile’s abuse department to request takedowns – whether by SRA or DMCA -- and have commended Hotfile’s responsiveness. (HF Facts 7,11.) *See pp. 6-8, supra.*

D. Hotfile Adopted And Reasonably Implemented An Appropriate Repeat Infringer Policy As Of February 18, 2011.

“[A] service provider ‘implements’ a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications....The statute permits service providers to implement a variety of procedures, but an implementation is reasonable if, under ‘appropriate circumstances,’ the service provider terminates users who repeatedly or blatantly infringe copyright.” *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109-10 (9th Cir. 2007); 17 U.S.C. § 512(i)(1)(A); *Ellison v. Robertson*, 357 F.3d 1072, 1080 (9th Cir. 2004).

Hotfile’s notification system and procedure for dealing with DMCA notices (including its SRA) have been exemplary. *See pp. 7-8 and 15-16, supra.* Hotfile has never “actively prevent[ed] copyright owners from collecting information needed to issue such notifications,” and its expeditious response is not disputed. *CCBill*, 488 F. 3d at 1109. *See also Io*, 586 F. Supp. 2d at

1143 (safe harbor where “policies have identified its designated Copyright Agent to receive notification of claimed violations,” Veoh “often responds to infringement notices the same day they are received, or at most, within a few days,” and it had “hash” fingerprinting); and *Viacom*, 718 F. Supp. 2d at 524 (removal of all links by “next business day”).

There can be no dispute that Hotfile has “informed subscribers and account holders” of its repeat infringer policy. *CCBill*, 488 F.3d at 1109. See pp.6-8, *supra*. (HF Fact 5.) *Corbis*, 351 F. Supp. 2d at 1101-02 (policy “need only put users on notice that they face exclusion from the service if they repeatedly violate copyright laws”; no need to reveal internal decision-making criteria). Its Intellectual Property Policy Page unambiguously advises:

It is Hotfile’s policy to: (1) accommodate and not interfere with standard technical measures (as defined by the DMCA) used to identify and protect copyrighted works; (2) disable access to or remove content that it believes in good faith may infringe the copyrights of third parties; and (3) **discontinue service to users who repeatedly make such content available or otherwise violate HotFile’s Terms of Service.** Please do not abuse the HotFile service by using it to distribute materials to which you do not have the rights.

(HF Fact 5) (emphasis added).

Since the outset, Hotfile has identified and terminated “users who repeatedly or blatantly infringe copyright.” *CCBill*, 488 F.3d at 1109. In its initial startup period through early 2011, Hotfile’s policy was to terminate particular users who were identified by content owners as repeat infringers within Hotfile’s discretion. (Exhibit B ¶ 31.) Hotfile records confirm that over forty users were terminated under this policy in the pre-Complaint period, and many more than that were terminated but not recorded in Hotfile’s database. *Capitol Records*, 2011 WL 5104616, *7 (153 terminations of blatant infringers reasonable). The Studios did not once before filing this Complaint ask Hotfile to strengthen or alter its policy. (Exhibit B ¶ 32.) Nevertheless, because there are few guideposts in the case law on what is a reasonable policy under ‘appropriate circumstances,’¹⁰ Hotfile is not seeking summary judgment for the period of time before it revamped the repeat infringer policy effective on February 18, 2011.

¹⁰ Congress left the specific requirements of a repeat infringer policy “loosely defined,” and thereby gave service providers flexibility. *Corbis*, 351 F. Supp. 2d at 1100-2; see also Nimmer § 12B.10[A][1] (repeat infringer provision is “amorphous”). “[S]ection 512(i) does not require service providers to track users in a particular way or affirmatively police users for evidence of repeat infringement.” *Io*, 586 F. Supp. 2d at 1145.

It was only when the Studios filed their Complaint that Hotfile first learned they were dissatisfied with its repeat infringer policy. Complaint ¶ 42. [REDACTED]

[REDACTED] (HF Facts 21-23.) *Io*, 586 F. Supp. 2d at 1143 (upholding strikes-based policy as a matter of law); *UMG Cir.*, 2011 WL 6357788, *5, n. 5 (not challenging Veoh's strikes based repeat infringer policy.); *Perfect 10, Inc. v. CCBill*, 340 F. Supp. 2d 1077, 1094 n.12 (C.D. Cal. 2004)(policy of terminating accounts "after 3 notifications is reasonable"), *rev'd on other grounds*, *CCBill*, 488 F.3d 1102 (remand to review non-party notices); *Viacom*, 718 F. Supp. 2d at 527-28. *Capitol Records*, 2011 WL 5104616, *5 ("In cases of video and file sharing sites, courts have found reasonable implementation where service providers terminated the accounts of users who had been warned yet continued to upload material that had been the subject of a takedown notice.") Given this plain precedent, Hotfile's current repeat infringer policy indisputably terminates users under "appropriate circumstances" and is therefore reasonable.¹¹

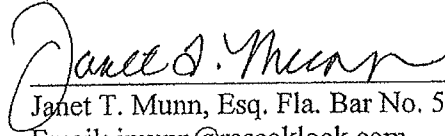
V. CONCLUSION

Hotfile has from its beginning complied with the letter and spirit of the DMCA. It has worked proactively with the Studios and other content owners to maximize the effectiveness of its copyright enforcement tools and procedures, as acknowledged by the Studios themselves. Hotfile is accordingly entitled to the DMCA safe harbor protection. The Court should grant Hotfile's motion for summary judgment as of February 18, 2011, the date on which Hotfile adopted its "three-strikes" repeat infringer policy. A Proposed Order is attached hereto as Exhibit C.

¹¹ The final requirement for safe-harbor protection is to accommodate and not interfere with "standard technical measures." 17 U.S.C. § 512(i)(1)(B). That is a defined term, which applies only to "technical measures ... used by copyright owners to identify or protect copyrighted works" that have been "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process," "are available to any person on reasonable and nondiscriminatory terms," "do not impose substantial costs on service providers or substantial burdens on their systems or networks." 17 U.S.C. § 512(i)(2); (S. Rep. No. 105-190, at 52, Ex. 1 to Exhibit A). The Studios make no allegation that Hotfile has not complied with this requirement, and there is no evidence to the contrary.

DATED: February 17, 2012

Respectfully submitted,



Janet T. Munn, Esq. Fla. Bar No. 501281

Email: jmunn@rascoklock.com

RASCO KLOCK

283 Catalonia Avenue, Suite 200

Coral Gables, FL 33134

Telephone: 305.476.7101

Telecopy: 305.476.7102

And



Roderick M. Thompson, Esq. (admitted *pro hac vice*)

Email: rthompson@fbm.com

Andrew Leibnitz, Esq. (admitted *pro hac vice*)

Email: aleibnitz@fbm.com

Anthony P. Schoenberg, Esq. (admitted *pro hac vice*)

Email: tschoenberg@fbm.com

Deepak Gupta, Esq. (admitted *pro hac vice*)

Email: dgupta@fbm.com

Janel Thamkul, Esq. (admitted *pro hac vice*)

Email: jthamkul@fbm.com

FARELLA BRAUN + MARTEL LLP

235 Montgomery St.

San Francisco, CA 94104

Telephone: 415.954.4400

Telecopy: 415.954.4480

And

Valentin Gurvits, Esq. (admitted *pro hac vice*)

Email: vgurvits@bostonlawgroup.com

BOSTON LAW GROUP

825 Beacon Street, Suite 20

Newton Center, MA 02459

Telephone: 617.928.1800

Telecopy: 617.928.1802

*Counsel for Defendants Hotfile Corporation
and Anton Titov*

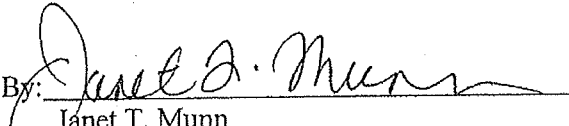
CERTIFICATE OF SERVICE

I hereby certify that on February 17, 2012, a true and correct copy of the foregoing document, was filed conventionally under seal and served on all counsel of record identified below via e-mail and via FedEx.

Karen L. Stetson, Esq.
GRAY-ROBINSON, P.A.
Email: Karen.Stetson@gray-robinson.com
1221 Brickell Avenue
Suite 1600
Miami, FL 33131
Telephone: 305.416.6880
Telecopy: 305.416.6887

Karen R. Thorland, Esq. (admitted *pro hac vice*)
Senior Content Protection Counsel
Email: Karen_Thorland@mpaa.org
Motion Picture Association of America, Inc.
15301 Ventura Boulevard, Building E
Sherman Oaks, CA 91403-5885
Telephone: 818.935.5812

Steven B. Fabrizio, Esq. (admitted *pro hac vice*)
Email: sfabrizio@jenner.com
Duane C. Pozza, Esq. (admitted *pro hac vice*)
Email: dpozza@jenner.com
Luke C. Platzer, Esq. (admitted *pro hac vice*)
Email: lplatzer@jenner.com
JENNER AND BLOCK, LLP
1099 New York Avenue, N.W.
Suite 900
Washington, DC 20001
Telephone: 202.639.6000
Telecopy: 202.639.6066

By: 
Janet T. Munn

APPENDIX A

**Pertinent Portions of Digital Millennium Copyright Act
17 U.S.C. § 512(C) - Safe Harbor for Storage At Direction of Users**

17 U.S.C. § 512

* * * *

(c) Information Residing on Systems or Networks at Direction of Users.—

(1) In general:— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright 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 -

(A)

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent. — The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification. —

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)

(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of

subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

* * * *

(i) Conditions for Eligibility.—

(1) Accommodation of technology. — The limitations on liability established by this section shall apply to a service provider only if the service provider —

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider’s system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

* * * *

(k) Definitions.—

(1) Service provider. —

(A) As used in subsection (a), the term “service provider” means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.