UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

REFX AUDIO SOFTWARE, INC., Plaintiff, vs. DOES 1-89, Defendants.	Case No.: TBD Judge: **JURY TRIAL DEMANDED**

PLAINTIFF'S MEMORANDUM OF LAW IN SUPPORT OF
APPLICATION FOR LEAVE TO TAKE IMMEDIATE DISCOVERY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

FEDERAL RULES

I. INTRODUCTION

Plaintiff reFX Audio Software Inc. ("reFX Audio" or "reFX"), a software developer and copyright-holder, alleges that 89 Doe Defendants infringed its copyrights in the Plaintiff's ROM synthesizer plug-in software, including, but not limited to, "Nexus 2" and "Nexus 2.2.0" (collectively, "Software"). Each Doe used an Internet file sharing protocol known as BitTorrent to copy and reproduce the Software over the Internet. Defendants' actions resulted in the unauthorized, viral dissemination and infringement of its Software. Despite Plaintiff's best efforts, at this time the infringing activity can only be identified by the IP address each Doe used to accomplish his or her acts of infringement. Plaintiff's investigator utilized geolocation technology which, upon information and belief, places each IP address in this suit within Connecticut.

Each IP address is assigned by an Internet Service Provider ("ISP") to an individual or corporate subscriber. These ISPs possess the information necessary to identify the subscribers with the IP addresses used by the Doe Defendants to infringe Plaintiff's copyrighted Software. The identity of each subscriber to whom such IP address has been assigned is necessary for the Plaintiff to proceed with this action.

Accordingly, Plaintiff seeks leave to serve limited discovery on the ISPs to determine the identity of each subscriber whose IP address has been used to infringe the Plaintiff's copyright in the Software. Plaintiff seeks information limited to documents, including electronically-stored information, sufficient to identify each subscriber's name, address where the IP address was located at the time of the infringement, telephone number, e-mail address(es), and Media Access Control ("MAC") addresses. Upon discovery of each subscriber's identity, Plaintiff intends to seek further discovery from those individuals or corporations to determine the identity of the

parties responsible for the illicit sharing of the copyrighted Software and infringement of Plaintiff's Software. With this information Plaintiff may then amend the Complaint to substitute the Doe Defendants.

II. ARGUMENT

a. Precedent Allows for Expedited Discovery to Identify the Doe Defendants.

The Second Circuit Court of Appeals and District Courts within this Circuit, including this Court, have routinely allowed discovery to identify "Doe" defendants. *See* Valentin v. Dinkins, 121 F.3d 72, 75-76 (2d Cir. 1997) (vacating dismissal; *pro se* plaintiff should have been permitted to conduct discovery to reveal identity of the defendant); John Wiley & Sons Inc. v. Doe Nos. 1-30, 12 Civ. 3782 (LTS)(JLC), (S.D.N.Y. May 31, 2012); Arista Records LLC, et al. v. Does 1-4, 589 F.Supp.2d 151 (D. Conn. Dec. 9, 2008) (allowing expedited discovery because "learning the true identities of the pseudonymous individuals alleged to have violated Plaintiffs' copyrights is essential to their prosecution of this litigation …." *Id.* at 153.). In actions against BitTorrent Defendants, District Courts within this Circuit have granted motions for such expedited discovery. *See* Digital Sin, Inc. v. Does 1-27, 12 Civ. 3873, 2012 WL 2036035 (S.D.N.Y. June 6, 2012) (herein "Digital Sin II"); Malibu Media, LLC v. Does 1-10, CV 12-1146, 2012 WL 1020455 (E.D.N.Y. Mar. 26, 2012); Digital Sin, Inc. v. Does 1-176, 279 F.R.D. 239 (S.D.N.Y. Jan. 30, 2012) (herein "Digital Sin I").

This Court has applied a good cause standard for expedited discovery in cases involving alleged copyright infringement by unnamed Doe Defendants. *Arista Records LLC*, 589 F.Supp.2d at 152-153 (allowing expedited discovery of "personally identifying information associated with the IP addresses [Plaintiff has] linked to each Defendant."). In *Arista Records*, this Court found good cause existed for expedited discovery of subscriber information from ISPs

where Plaintiff was able to show that 1) learning the identities of the individuals alleged to have violated Plaintiff's' copyrights was essential to prosecution, and 2) there would be little, if any, prejudice to the Defendants. *Id.*

Here, Plaintiff cannot move forward with prosecution of this litigation without learning the identities of the subscribers whose IP addresses were used by the Doe Defendants it alleges to have infringed Plaintiff's copyrights. In addition, the discovery requests have been narrowly tailored to include only enough information as necessary to sufficiently identify each IP address subscriber's name, current address where the IP address is located, telephone number, e-mail address(es), Media Access Control ("MAC") addresses and any policies and agreements governing the subscriber's use of the account and IP address, such as TOS, AUP and CIP, that were applicable to the subscriber and in effect at the time of the alleged infringement. Such requests do not prejudice the Doe Defendants in any way. In many instances the infringer is the account holder. In other circumstances a subscriber may be held responsible for the infringement committed by others using the internet connection and IP address assigned to the subscriber's account. This will be revealed in discovery.

b. Plaintiff Alleges Copyright Infringement and Contributory Copyright Infringement Based on Doe Defendants' BitTorrent Activity.

Here, the Doe Defendants used an online media distribution system called BitTorrent to download and distribute the copyrighted Software. Complaint at ¶ 4. Plaintiff engaged Copyright Defenders, Inc. ("Copyright Defenders") to monitor and stop this infringing activity. Declaration of Matthias Schroeder Padewet at ¶ 6.

i. Defendants' Infringing Activity

The Internet is a vast collection of interconnected communicating computers and networks. Padewet Decl. at ¶ 4. In allowing hundreds of millions of people around the world to freely exchange ideas and information, the Internet has afforded opportunities for the wide-scale infringement of copyrighted software. *Id.* As software exists in an unsecured digital format, it can be copied and distributed an unlimited number of times over the Internet. *Id.* To do this, many individuals use online media distribution systems or so-called "peer-to-peer" ("P2P") networks. *Id.* P2P networks are usually computer systems that enable Internet users to (1) make works stored on each user's computer available for copying by other users or peers; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another. *Id.*

Millions of people unlawfully use P2P networks to connect to other's computers to upload (distribute) and/or download (copy) copyrighted material. *Id.* at ¶ 5. These P2P systems cause a "viral" distribution of digital files: each user who copies a digital file from another user can then distribute the file to other users and so on. Padewet Decl. at ¶ 22. Here, Plaintiff observed infringement, but does not know the true identities of those committing the infringement. *Id.* at ¶¶ 23-25, 31. Infringement begins when an initial file-provider intentionally elects to share a file, called seeding, using a P2P network. *Id.* at ¶ 8. Other users ("peers") on the network connect to the seed file to download. *Id.* at ¶ 8. The P2P protocol at issue in this suit is called "BitTorrent." *Id.* at ¶ 19. What makes BitTorrent unique is that, as yet additional peers request the same file, each new user becomes a part of the network from where the file can be downloaded. *Id.* Unlike a traditional P2P network, each new downloader is receiving a portion of the data from each connected user who has already downloaded a part of the file that together comprises the whole. *Id.* Thus, every peer who has a copy of the infringing

copyrighted material on a P2P network investigated by Copyright Defenders' software is also a source of download for that infringing file. Padewet Decl. at ¶ 9.

To have engaged in the Software's distribution, each participating peer intentionally obtained a torrent file for the Software from a BitTorrent or torrent website. *Id.* at ¶ 16. Each peer then loaded that torrent file into a computer program that reads such files. *Id.* at ¶ 16. Once loaded the BitTorrent program employed a protocol to initiate simultaneous connections to hundreds of other peers possessing and sharing copies of the Software described in the file. *Id.* at ¶ 16. Once connected, the program coordinated the copying of the Software among participating peers. *Id.* at ¶ 17. As the Software was copied to the peers' computers piece by piece, the downloaded pieces were immediately available to others seeking the file. *Id.* at ¶ 17.

Torrent files contain a unique hash identifier generated by a mathematical algorithm. Padewet Decl. at ¶ 13. These files have unique "info-hashes" which act as "roadmaps" to the addresses of other users who are sharing these media files and specifics about those media files. *Id.* The hash identifier of the torrent file utilized by peers to distribute and share Plaintiff's Software is **1DCAAFEA49753AF5A83ACBFD9022762138E5CDBD** ("Hash 1DCA") *Id.* Each peer is a member of one "swarm" (i.e., group of BitTorrent peers); the swarm members were collectively connected to share the particular hash file (here, the Hash 1DCA file containing the Software), and this swarm is associated with only one hash identifier, Hash 1DCA. *Id.* at ¶ 18. Each peer participated in the swarm to reproduce and distribute the Software. *Id.* at ¶ 21.

Posing as a member of the swarm, Plaintiff's investigators tracked the swarm members uploading and sharing the Software. *Id.* at ¶ 23. Investigators then downloaded parts of the Software from the tracked swarm members and stored information specific to each download,

including the date and time of the activity and the IP address used by each swarm member to facilitate the copying and distribution of the Software. Padewet Decl. at ¶¶ 23, 25. Each of the swarm members tracked by Plaintiff's investigators made available unauthorized pirated copies of Plaintiff's copyrighted Software to other users via BitTorrent, including Plaintiff's investigators. *Id.* at ¶ 23. Each of the tracked swarm members have chosen not only to infringe by downloading a pirated copy of Plaintiff's copyrighted Software but also by re-publishing, distributing and sharing the pirated copy with other members of the swarm. *Id.* at ¶ 22.

The terms of each service agreement and acceptable use policy for each of the respective ISPs specifically state that the subscriber is responsible and liable for any and all use of the subscriber's IP address, including violation of copyright laws, by any and all users of the subscription account and IP address.

The acceptable use policies put each subscriber on notice that the subscriber shall not allow use of the account and IP address to infringe the intellectual property rights of third parties and, as a result, the terms of service also provide notice to the subscriber that he will be held responsible for all use which causes infringement of third party rights.

For example, Cablevision's Terms of Service ("TOS") for its Optimum Online Internet access service (http://www.optimum.net/Terms/) (attached as Exhibit 1) defines Subscriber as the person in whose name the account is registered, all members of that person's household and any other user of the Service:

> **Subscriber or User**: Each member of your household and any other individual who uses the Computer and Optimum Online irrespective of the individual in whose name the account is in or who owns, rents or uses the premises on which the Computer is located.

The TOS further provides that the subscriber is acknowledging the TOS on behalf of him or herself and all members of the household and anyone else who uses the computer devices

attached to the network and which gain access to the internet through by means of the devices assigned the IP address (e.g., modem, router, etc.):

> **Multiple Users**: Subscriber acknowledges that by "clicking" the Acceptance icon below and/or by using the Optimum Online Service, Subscriber is agreeing to the terms and conditions of this Agreement on behalf of all persons who use the Optimum Online Service or the Services through Subscriber's Computer or other devices. Subscriber shall be responsible for ensuring that all Subscribers understand and comply with the terms and conditions of this Agreement. Subscriber acknowledges and agrees that the Subscriber is responsible and liable for any and all breaches of the terms and conditions of this Agreement, whether such breach is the result of use of the Optimum Online Service or Services.
>
> *Id.*

Of course, the Subscriber also agrees to abide by Cablevision's Acceptable Use Policy ("AUP") (http://www.optimum.net/Privacy/AUP) (attached as Exhibit 2):

> **Acceptable Use Policy**: Subscriber shall comply with all of Cablevision's standards for acceptable use with respect to the Optimum Online Service and the Services and shall refrain from any and all illegal and/or inappropriate activities, including without limitation as outlined in the Acceptable Use Policy. The Cablevision Internet Product Acceptable Use Policy will be updated from time to time and the latest version will supersede all prior versions. Please click here for the most updated Acceptable Use Policy.

Subscribers are placed on notice that they must employ security on their networks and abide by the AUP:

> **Security**: Users must adhere to the Optimum Online security policies set forth in the Acceptable Use Policy.
>
> Cablevision reserves the right to protect the integrity of its network and resources by any means it deems appropriate. This includes but is not limited to: monitoring traffic, port blocking, e-mail virus scanning, denying e-mail from certain domains, and putting limits on bandwidth and e-mail.
>
> Subscriber is solely responsible for any misuse of the Optimum Online Service or the Services, as well as for the security of any device you choose to connect to the Optimum Online Service, including any data stored on that device, all as detailed more fully in the Acceptable Use Policy.
>
> Subscriber is solely responsible for maintaining the security of Subscriber's

> computer(s), devices and data, including without limitation, encryption of data and protection of Subscriber's Optimum ID, password and personal and other data. If Subscriber believes his/her login credentials have been lost or stolen, or that someone has gained access to his/her account or login credentials without Subscriber's permission, please contact us at abuse@cv.net.
>
> *Id.*

Importantly, the TOS clearly state that the Subscriber take care not to allow the account to be used to infringe the intellectual property rights of third parties, and incorporates Cablevision's Copyright Infringement Policy ("CIP") (http://www.optimum.net/Privacy/Copyright) (attached as Exhibit 3):

> **Inappropriate Content**: Subscriber also agrees not to store, distribute or otherwise disseminate any material or content over the Optimum Online Service in any manner that constitutes an infringement of third party intellectual property rights, including but not limited to copyrights. Cablevision reserves the right to take action at its own discretion and as required by the Digital Millenium [sic.] Copyright Act, any other applicable laws, rules or regulations, or court order including but not limited to termination of a Subscriber's access to the Optimum Online Service. Alleged infringements will be handled in accordance with Cablevision's Copyright Infringement Policy.

Of course, the AUP clearly puts the Subscriber on notice that the Service cannot be used to infringe the intellectual property rights of third parties:

> **Illegal Use**: The Service may be used only for lawful purposes. Transmission or distribution of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene, illegal, defamatory, constitutes an illegal threat, or violates export control laws. Your use of the Service is also subject to Cablevision's Copyright Infringement Policy. Furthermore, use of the Service to impersonate a person or entity is not permitted.
>
> Exh. 2.

The TOS for the various BitTorrent client software applications similarly contain express provisions restricting use of the service, and provide ample notice that the software is

not to be used to infringe the intellectual property rights of third parties. *See, e.g.*, http://www.vuze.com/corp/terms.php. Attached hereto as Exhibit 4. By the same token, the clear and overwhelming reason infringers choose BitTorrent protocol to download, publish and share files is that the client software engages in automatic uploading using the same computers connected to the internet via the IP address. As stated in the BitTorrent End User License Agreement ("EULA") (http://www.bittorrent.com/legal/eula) (attached as Exhibit 5):

> **Automatic Uploading**: The Software accelerates downloads by enabling your computer to grab pieces of files from other BitTorrent users simultaneously. Your use of the Software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In the Software, only files that you are explicitly downloading or sharing or have downloaded or shared through BitTorrent will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall the Software through the Add/Remove Programs control panel utility. In addition, for the BitTorrent or uTorrent software, you can control the Software in multiple ways through its user interface without affecting any files you have already downloaded.

Finally, ISP account holders are clearly provided notice they will be held responsible for any conduct occurring over their subscription account and IP address, regardless of whether committed by the account holder (Subscriber or User under the AUP and TOS), or a third party with access to the account. As stated in Cablevision's AUP:

> **User Responsibility**: Users are solely responsible for the security and misuse of any device that is connected to the Service, regardless of whether the misuse was committed by the User or a third party with access to the User's Service account. Cablevision recommends that Users implement appropriate measures to secure their systems and these measures may include installation of firewalls, antivirus protection with regular updates, regularly checking for and applying security patches for software and operating systems, and general security conscience use of the Service. Further, the speed at which a User connects to the Internet is dependent upon many factors, including a User's hardware and software and the activities in which the user is engaging. Cablevision does not guarantee or warrant any particular speed of Internet connection.
>
> Exh. 2.

ii. Preliminary Identification of Defendants.

Padewet engaged in a process to identify direct infringers of Plaintiff's copyright and identified all Defendants in the following manner. Padewet Decl. at ¶ 6. The specially designed software used by Padewet connected to a number of files of unauthorized versions of the Software. *Id.* at ¶ 24. All infringers connected to those files were investigated through downloading a part of the file placed on their computer. *Id.* This evidence is saved on Padewet's server and can be shown to the court as evidence if necessary. *Id.*

Once the searching software identified a user offering the file for download, the software obtained that user's IP address. *Id.* at ¶ 25. In addition to the Software file, Padewet downloaded or otherwise collected publicly available information about the network user that is designed to help it identify the infringer. *Id.* at ¶ 25. Among other things, Padewet downloaded or recorded for each file downloaded: a) the time and date at which the file or a part of the file was distributed by the user; b) the IP address assigned to each user at the time of infringement; c) the ISP for each defendant; and, in some cases, d) the Software file's metadata (digital data about the file); e) the BitTorrent client application (program) used by each user, f) the global unique identifier for each file downloaded by each user, and g) the location of most users (by city and state) at the time of download, as obtained by geolocation technology. *Id.* at ¶ 25. Evidence logs are created for each user and this information is stored in a database. Padewet Decl. at ¶ 25.

An IP address is a unique identifier that an ISP assigns to a user. *Id.* at ¶ 28. Each time a subscriber logs on, he or she may be assigned a different IP address unless the user obtains a static IP address. ISPs track the IP addresses assigned to subscribers and retain "user logs" for a limited time. *Id.* at ¶ 28. These logs provide the most accurate means to connect an infringer's identity to its infringing activity. *Id.* at ¶ 28. Although users' IP addresses are not automatically displayed on P2P networks, any user's IP address is identifiable from exchanged packets of data.

Id. at ¶ 29. The manner in which a user's IP address is determined varies by P2P network. *Id.* at ¶ 29.

An infringer's IP address is significant because it becomes a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer. Padewet Decl. at ¶ 30. However, the IP address alone does not enable Plaintiff to ascertain with certainty the exact physical address of the computer or to determine the infringer's identity. *Id.* It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP and, in some instances, to a general geographic area. *Id.*

Here, the identified IP addresses enable Plaintiff to determine which ISP was used by each infringer to gain access to the Internet. *Id.* at ¶ 31. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. *Id.* However, some ISPs lease or otherwise allocate certain IP addresses to unrelated, intermediary ISPs. *Id*. Since these ISPs have no direct relationship — customer, contractual, or otherwise — with the end-user, they are unable to identify the Doe Defendants through reference to their user logs. Padewet Decl. at ¶ 31. The intermediary ISPs' own user logs, however, should permit identification of the subscribers and, in turn, the Doe Defendants. *Id.* Plaintiff, through its investigations, has determined that the Doe Defendants here were using the ISPs listed in Exhibit A to Plaintiff's Complaint together with various other ISPs, to gain access to the Internet via the IP addresses to distribute and make available the Software for distribution and copying. *Id.*

iii. Plaintiff's Confirmation of Copying.

Plaintiff confirmed the files it downloaded were actual copies of the Software through a visual comparison between downloaded file and the work itself. *Id.* at ¶ 34. As to Plaintiff's

copyrighted Software, Padewet or one of his assistants visually compared the downloaded file with the original Software to confirm infringement. *Id.* at ¶ 35.

iv. The Specific Information Plaintiff Seeks.

Exhibit A to the Complaint provides the Court with the IP addresses utilized by each Doe Defendant to infringe the Plaintiff's copyright in the Software and the ISP responsible for each IP address. Complaint at ¶ 18 and Exhibit A. This data constitutes the information obtained up to the date of the filing of the Complaint. Plaintiff specifically requests leave to obtain discovery from the ISPs in order to learn the identities, including name and contact information, of the account holders whose IP addresses were used by Doe Defendants to illegally download and distribute Plaintiff's copyrighted Software as well as the MAC addresses which will reveal the computers connected to each IP address that were used in the unauthorized distribution of Plaintiff's Software. Plaintiff also requests the policies and agreements (including TOS, AUP and CIP) in effect at the time of the alleged infringement.

Using its best investigative efforts, Plaintiff has been able to identify at least the following information regarding each Doe Defendant: a) the time and date at which the file or a part of the file was distributed by the Doe Defendant; b) the IP address utilized by the Doe Defendant at the time of infringement, and c) the ISP providing service to the each Doe Defendant at the time of infringement, and, in some cases, d) the program file's metadata, e) the BitTorrent client application used by each Doe Defendant, the global unique identifier for each file downloaded by each Doe Defendant, and g) the location of the Doe Defendants at the time of download. Padewet Decl. at ¶ 25. This information, while useful, does not reveal the identity of the Doe Defendants. In order to determine the identities of each Doe Defendant Plaintiff requires information only available from the ISPs, including basic account holder information as

well as the TOS, AUP, and CIP agreements in effect at the time of the infringement. This information will allow Plaintiff to conduct limited additional discovery upon the identified account holders in order to determine the true identity of the Doe Defendants.

c. Good Cause Exists for the Expedited Discovery.

The District of Connecticut has considered three factors to determine whether good cause exists for expedited discovery to identify anonymous Internet users: 1) irreparable harm from infringement; 2) no prejudice to the defendants; 3) forward movement of the case. *Arista Records*, 589 F.Supp.2d at 152-153. Plaintiff easily meets these three factors.

i. Plaintiff Suffers Irreparable Harm from the Past and Ongoing Infringement of the Copyrighted Software.

Plaintiff has suffered and will continue suffering irreparable harm from the unauthorized copying and distribution of its Software. The elements of copyright infringement are 1) ownership of a valid copyright and 2) copying of the protectable elements of the copyrighted work. Scholz Design, Inc. v. Sard Custom Homes, LLC, 691 F.3d 182, 186 (2d Cir. 2012). Plaintiff's copyrights in the Software are valid. Complaint at ¶¶ 38-41 and Exhibits B and C; *see also* 17 U.S.C. § 410(c).

Copyright infringement may be proven by showing that a defendant had access to the copyrighted material and that substantial similarity exists between the infringing work and the copyrighted work. Folio Impressions, Inc. v. Byer California, 937 F.2d 759, 765 (2d Cir. 1991). Defendants here had access to the Software in question: it is a popular program, particularly among BitTorrent users. Metro-Goldwyn-Mayer, Inc. v. Am. Honda Motor Co., 900 F. Supp. 1287, 1297 (C.D. Ca1. 1995) ("sheer worldwide popularity and distribution" of a copyrighted work allows the Court to presume access to said work) *citing* Warner Bros., Inc. v. American

Broadcasting Companies, Inc., 654 F.2d 204 (2d Cir. 1981). Plaintiff's investigations also confirmed each Doe Defendant's access to the works in questions and Plaintiff's investigators confirmed the files downloaded were, in fact, Plaintiff's Software.

Substantial similarity exists between the copyrighted works and the allegedly infringing works. Padewet Decl. at ¶¶ 34-35. The hash file at issue provided access to an unauthorized copy of Plaintiff's copyrighted Software. Complaint at ¶¶ 13, 49-51. Copyright Defenders visually compared the program downloaded from the hash file with the copyrighted Software. Padewet Decl. at ¶¶ 34-35. Plaintiff's investigators confirmed that the material downloaded from the hash file contains a substantial portion of the copyrighted Software. *Id.*

Despite Plaintiff's exclusive ownership, Defendants are engaged in a joint act of infringement — each Doe used BitTorrent to copy and reproduce the Software resulting in its unauthorized dissemination. As a result of this infringement, Plaintiff suffered and continues to suffer from lost sales and Plaintiff is entitled to injunctive relief as well as statutory damages and other remedies. 17 U.S.C. §§ 502-505. Plaintiff further states a *prima facie* claim for contributory copyright infringement. Each defendant was a willing and knowing part of the swarm for purposes of infringing conduct. Complaint at ¶¶ 53, 55-61.

ii. The Expedited Discovery will Cause no Prejudice to Defendants.

Plaintiff seeks contact information for the individual subscribers whose IP addresses were used by Doe Defendants to copy and distribute Plaintiff's Software. Because of the partially anonymous nature of Defendants' distribution system, Plaintiff's investigators have been unable to determine the Does' names and addresses. Padewet Decl. at ¶¶ 30-31. Plaintiff now seeks this limited information from the ISPs. The discovery is narrowly tailored to obtain only the information required. *Arista Records*, 589 F.Supp.2d at 152-3. Discovery of this information

will not prejudice defendants; Plaintiff will use this information for the limited purpose for enforcing its copyrights and prosecution of this lawsuit.

iii. The Forward Movement of the Case Turns on the Information Sought by the Expedited Discovery, which has Limited Availability.

As set forth above, each ISP assigns a unique IP address to each subscriber and keeps track of the IP addresses for these subscribers. Padewet Decl. at ¶ 28. The subscriber information for each IP address utilized by the Doe Defendants is within the custody and control of each subscriber's ISP. *Id.* Because ISPs provide a service to subscribers, *i.e.*, provide an IP address for Internet access, the ISPs must maintain contact information and billing records for each subscriber in order to receive compensation for such services. *Id.* Thus, these ISPs can provide this identifying information to Plaintiff. *Id.* at ¶ 31.

In *Digital Sin I,* the court found Plaintiff had no other way of obtaining the identities of BitTorrent infringers other than expedited discovery. *Digital Sin I,* 279 F.R.D. at 241-242. Specifically, "absent a Court-ordered subpoena, many of the ISPs ... are effectively prohibited by 47 U.S.C. § 551(c) from disclosing the identities of the putative defendants to Plaintiff." *Id.* In fact, the *Digital Sin I* court recognized that there is no other indication or ruling in any other court throughout the country "that the plaintiffs have any reasonable alternative to these subpoenas to obtain the identities of the alleged infringers." *Id.* Even further, "without granting plaintiff's request, the defendants cannot be identified or served and the litigation cannot proceed." *Id.*

Expedited discovery is necessary because IP data can be lost forever due to routine deletion by ISPs. *Id.* Plaintiff will be irreparably harmed should the IP data held by the ISPs be deleted because Plaintiff has no other method available to identify the Doe Defendants sufficient to prosecute the claims.

d. The Discovery Sought is Proper as to All Doe Defendants.

Rule 20(a)(2) of the Federal Rules of Civil Procedure allows multiple defendants to be joined in one action. Rule 20 is a two-prong test that allows joinder when: 1) claims arise out of the same transaction, occurrence or series of transactions and 2) there is at least one common question of law or fact linking all of the claims. Malibu Media, LLC v. John Does 1-5, 83 Fed. R. Serv. 3d 593 (S.D.N.Y. Aug. 24, 2012) ("[B]ecause of the nature of the BitTorrent protocol, each defendant's participation in the swarm facilitated, even if only indirectly, the participation of the other defendants who followed in time." *Id.* at *3.).

District courts should take a liberal approach to permissive joinder. United Mine Workers v. Gibbs, 383 U.S. 715, 724 (1966). In the recent case of *Malibu Media, LLC v. John Does 1-5*, the Southern District of New York ruled that joinder is appropriate for cases involving the BitTorrent protocol where Doe Defendants have both uploaded and downloaded pieces of copyrighted materials regardless of the length of time the Doe Defendants were alleged to have participated in the swarm. *Malibu Media*, 83 Fed. R. Serv. 3d 593, at *3-4 (S.D.N.Y. Aug. 24, 2012) ("[T]he BitTorrent protocol operates such that every user is logically related to every other user who participates in the same swarm, regardless of their time of participation.").

i. Each Doe Defendant Participated in the Same Transaction or Occurrence or Series of Transactions.

All Defendants in this suit acted within one swarm to copy and reproduce the Software. Each defendant's activity was part of the same transaction, occurrence, or series of transactions.

> ...it is difficult to see how the sharing and downloading activity of BitTorrent — a series of individuals connecting either directly with each other or as part of a chain or "swarm" of connectivity designed to illegally copy and share the exact same copyrighted file — could *not* constitute a "series of transactions or occurrences" for purposes of Rule 20(a).

Digital Sin I, 279 F.R.D. 239, 244. Other courts agree:

> ...joinder [is] appropriate at this early stage of litigation because the plaintiff asserts a right to relief against all Doe defendants that appears, given the technology involved, to arise out of the same series of transactions or occurrences and because common questions of law or fact seem to be raised with respect to all Doe defendants by virtue of the use of BitTorrent to transmit the same copy of the plaintiff's Work.

Raw Films, Ltd. v. John Does 1-15, 2012 WL 1019067, at *2-3 (E.D. Pa. Mar. 26, 2012).

> ...each unknown individual is a possible source and may be responsible for distributing the movie to the other unknown individuals, who are also using the same file sharing protocol to copy the identical copyrighted material.

AF Holdings v. Does 1-1,058, 2012 WL 3204917, at *12 (D.D.C. Aug. 6, 2012).

BitTorrent filing sharing is inherently suitable to the joinder analysis: "the pieces of the Work copied by each defendant may have been transmitted by or subsequently sent to other defendants, albeit indirectly, because recipient peers ... automatically begin delivering the piece they just received to other peers in the same swarm." *Raw Films*, 2012 WL 1019067, at *4 (citations omitted). A link exists even absent direct interaction among swarm members:

> Even if no Doe defendant directly transmitted a piece of the Work to another Doe Defendant, the Court is satisfied that at this stage of the litigation the claims against each Doe Defendant appear to arise out of the same series of transactions or occurrences, namely, the transmission of pieces of the same copy of the Work to the same investigative server.

Id. Such analysis applies even to a broad time frame of IP addresses. *AF Holdings*, 2012 WL 3204917, at *12 (holding there is no basis to rebut, at an early stage, that IP addresses identified as infringing four months apart were, at least potentially, part of the same swarm and provided or shared pieces of the plaintiff's copyrighted work.).

As set forth above, each Doe Defendant intentionally logged into a BitTorrent client repository, obtained a torrent file for Plaintiff's Software, loaded the file into a computer program, initiated simultaneous connections with other users and shared copies of the file for Plaintiff's Software, including with, upon information and belief, other identified Doe Defendants. Padewet Decl. at ¶¶ 10-18; Complaint at ¶¶ 48-51. The program coordinated the

piece by piece copying of Plaintiff's Software, and these downloaded pieces were then immediately available to all other members of the swarm, including the other Defendants in this action. Padewet Decl. at ¶ 17; Complaint at ¶ 51. These actions formed a single swarm among the 89 Defendants. Complaint at ¶¶ 52-53 and Exhibit A. Each of the peers is a member of this single swarm, connected for the purpose of sharing of the particular hash file and for the purpose of the reproduction and distribution of Plaintiff's copyrighted Software. Padewet Decl. ¶ at 21; Complaint at ¶ 55. Thus, Defendants acted in concert in effectuating the unauthorized copying, distribution and sharing of Plaintiff's copyrighted Software. Geolocation technology places all of the Doe Defendants in Connecticut. Complaint at ¶ 18 and Exhibit A.

Many Doe Defendants also acted in concert with other Doe swarm members by "Peer Exchange." Padewet Decl. at ¶ 19; Complaint at ¶ 57. Peer Exchange is a communications protocol built into almost every BitTorrent protocol which allows swarm members to share files more quickly and efficiently. Padewet Decl. at ¶ 19; Complaint at ¶ 57. Doe Defendants also likely acted in concert with other Doe swarm members by linking together globally through use of a Distributed Hash Table which is a sort of world-wide telephone book, which uses each file's "info-hash" (a unique identifier for each torrent file) to locate sources for the requested data. Padewet Decl. at ¶ 20; Complaint at ¶ 58. In doing so, swarm members rely on individual computers, rather than a central "tracker" computer, such that every client sharing this data is also helping to hold this worldwide network together. *Id.*

The nature of the BitTorrent protocol shows that Doe Defendants not only directly infringed Plaintiff's copyrights, but also contributed to the infringement of other members of the swarms. For example, Doe number 3 of Connecticut was a participant in Hash 1DCA and related swarm at least on January 22, 2013. Complaint at Exhibit A. Because of the collective

and interdependent nature of the BitTorrent protocol, Doe number 3's participation on January 22, 2013 strengthened the 1DCA swarm for all subsequent participants. *Id.*

Just as in *Malibu Media,* Plaintiff's right to relief, given the technology involved, arises out of the same series of transactions or occurrences. Even where courts have found that BitTorrent activity does not arise out the same series of transactions or occurrences, Rule 20 joinder is proper in that plaintiff has sufficiently pled 'shared, overlapping facts,' giving rise to Plaintiff's claims of infringement to make joinder presently proper." Third Degree Films v. Does 1-36, 2012 WL 2522151, at *9 (E.D. Mich. May 29, 2012) (*quoting* In re EMC Corp., 677 F.3d 1351, 1359 (Fed. Cir. May 4, 2012)).

ii. There are Questions of Law or Fact Common to All Defendants.

The second requirement of Rule 20 joinder is that a question of law or fact common to all of the defendants will arise in the action. *Malibu Media,* 83 Fed. R. Serv. 3d at *3. Rule 20(a) allows joinder of parties where "any question of law or fact common to all defendants will arise in the action." *Id. citing* Fed. R. Civ. P. 20(a)(2). The *AF Holdings* court recently supported joinder under this element, finding "At this procedural juncture, the claims against the unknown individuals infringing the plaintiff's copyright are identical." *AF Holdings,* 2012 WL 3204917, at *13. The *Raw Films* court agreed, stating "common questions of fact are likely to arise along with the legal standards for direct and contributory copyright infringement liability." *Raw Films,* 2012 WL 1019067, at *4. Indeed, in a similar motion for expedited discovery, the *Malibu Media* court in the Southern District of New York recently held "it is not in dispute that the claims against defendants present common questions of law or fact, thereby satisfying the second of the Rule 20(a)(2) criteria." *Malibu Media,* 83 Fed. R. Serv. 3d at *4.

Here, each defendant is accused of unlawfully copying the same Software and utilizing a single hash identifier to obtain and share his or her copy. Padewet Decl. at ¶¶ 16-18, 21; Complaint at ¶¶ 49-51. The hash identifier provides access to a copy of the copyrighted Software. Padewet Decl. at ¶ 13; Complaint at ¶ 14. These common questions of fact are sufficient for joining all defendants. Patrick Collins, Inc. v. Does 1-2,590, 2011 WL 4407172, at *6 (N.D. Cal. Sept. 22, 2011). Also, each defendant utilized BitTorrent protocol to obtain unlawful copies, and Plaintiff utilized a common investigation technique to identify each infringer and collect evidence regarding all Doe Defendants' infringing activities. *Id.; see* Padewet Decl. at ¶ 24. These factual issues will be essentially identical for each defendant. *Patrick Collins,* 2011 WL 4407172 at *6; Padewet Decl. at ¶ 24. While each defendant may later present different factual and substantive legal defenses, "this does not defeat, at this stage of the proceedings, the commonality in facts and legal claims that support joinder under Rule 20(a)(2)(B)." *Patrick Collins,* 2011 WL 4407172 at *6 (*quoting* Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332, 343 (D.D.C. Mar. 22, 2011).

iii. There is no Prejudice to any Party or Needless Delay.

Joinder of defendants who infringed the same copyrighted material promotes judicial efficiency. *Id.* at *7; *see also* London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 161 (D. Mass. 2008). The District of Columbia recently agreed:

> ...joinder of the claims against the unknown individuals associated with the Listed IP Addresses at this procedural juncture presents the most efficient mechanism for the plaintiff to obtain the identifying information required to evaluate the claims against each individual, protect its copyrighted work, and for judicial review of the plaintiff's claims.

AF Holdings, 2012 WL 3204917, at *11. The Defendants are currently not identified by name. Thus, they are not yet required to respond to Plaintiff's allegations, to assert a defense, or to oppose Plaintiff's motion for leave to take discovery. *Patrick Collins,* 2011 WL 4407172, at *7.

The Doe Defendants cannot show any harm or prejudice as a result of this Court granting the limited and narrowly tailored expedited discovery requested by Plaintiff.

III. CONCLUSION

Plaintiff reFX Audio Software Inc. respectfully seeks leave of Court to serve limited discovery on non-party ISPs as indicated in the attached proposed discovery order.

Respectfully Submitted,

By: /s/ Matthew C. Wagner

Matthew C. Wagner (ct25926)
mwagner@dmoc.com
Scott M. Harrington (ct02482)
sharrington@dmoc.com
Jonathan R. Longobardi (ct29032)
jlongobardi@dmoc.com
DISERIO MARTIN O'CONNOR & CASTIGLIONI, LLP
One Atlantic Street
Stamford, CT 06901
Telephone: (203) 358-0800
Facsimile: (203) 348-2321
Attorneys for Plaintiff

Dated: March 8, 2013