James S. Davis CALBAR NO.207963
Email: Jamesdee3080@msn.com
James S. Davis Attorney at Law
730 Broadway, Suite 102
Chula Vista CA 91910
(619) 934-4600
Of attorneys for plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DALLAS BUYERS CLUB, LLC, a Texas Limited Liability Company, Plaintiff, v. **DOE-69.181.52.57** Defendant.	Case No.: 3:16-cv-01164-JSC MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO ISSUE AN FRCP 45 SUBPOENA FOR DEPOSITION

INTRODUCTION

In July 2015, counsel for Plaintiff started filing copyright infringement cases in the state of California. In preparing to pursue claims on behalf of independent motion picture studios, counsel researched the past history of this type of litigation. What became apparent was a history of abuse of the system by a "porn-trolling collective," commonly known as Prenda, and described by Judge Wright as taking advantage of the copyright laws to "plunder the citizenry." In these cases, Plaintiffs would offer settlements for a sum calculated to be just below the cost of defense, creating a situation in which a Defendant would reluctantly pay rather than have their names associated with illegally downloaded porn. *Ingenuity 13, LLC v. John Doe*, 2:12-cv-8333, C.D. Cal., May 6, 2013, Judge Otis D. Wright, Sanctions Order. This was a pattern of clear abuse and is well recognized.

As a result of the actions by the "porn-trolling collective," an aggressive BitTorrent Defense Bar, whom is against any copyright enforcement, has attempted to have all copyright enforcement actions categorized as part of the "porn-trolling collective" through the use of the internet with sites like, dietrolldie.com, torrentfreak.com, fightcopyrighttrolls.com, and related arguments presented to the courts. In some countries this opposition is organized as a political party called the Pirate Party[1], but domestically often referred to as the Copyleft. This BitTorrent Defense Bar is critical of any copyright enforcement actions without regards to any specifics. A settlement demand that is too high would be unfair extortion, one that is too low would be exploiting the costs of litigation and extracting mere nuisance value. A plaintiff that dismisses a case is accused of running away from a fight and refusing to litigate, and one that responds to a motion is leveraging litigation costs and imposing an unfair burden on a defendant driving up costs.

In pursuing these matters on the behalf of clients, counsel has attempted to be transparent in working with this Court, and other courts, in the enforcement of clients' copyrights and implementing a litigation strategy to stop the practice of seeding or distributing their works. In effecting a strategy, counsel has and continues to collaborate and work with counsel of other states who have worked with courts, and through trial and error, found the best methods to create a fair and reasonable vehicle for legitimate motion pictures studios to enforce their copyrights and stop the seeding and distribution of their motion pictures.

In particular, counsel for Plaintiff, has worked with counsel from Oregon, who has worked with the Oregon District Court in tailoring a system for early discovery in these cases that has become fair, effective, and cost efficient for all parties involved. In creating the system currently in use, the Oregon District Court looked at a number of factors which included, the need of discovery for plaintiffs, the protection and inconvenience of a subscriber, legitimate concerns identified by the BitTorrent Defense Bar, and experience of hundreds of cases.

[1] https://en.wikipedia.org/wiki/Pirate_Party

As a result, after hundreds of cases, many of them by DBC, the District of Oregon saw through the hype and after 3 years of observation, in 2016, instituted Standing Orders to govern these types of cases. They found it necessary to caution defendants and some defense counsel that, "contrary to information available through the Internet" these cases are real, and plaintiff's claims are legitimate. Exhibit 1, D. Or. Standing Order 2016-7; See also Exhibit 2, D. Or. Standing Order 2016-8, granting initial discovery automatically and an initial 2 hour FRCP 45 deposition of any identified subscriber.

Plaintiff's demonstrated strategy is to:

1) Identify IPA's that are confirmed as distributing Plaintiff's motion picture at a high level through the BitTorrent distribution system, often persistently for weeks or even months. These are the parties that are not simply downloading a motion picture, but are regularly distributing or "seeding" motion pictures to others. At any one time there are tens of thousands of infringers in this District. Plaintiff directs its actions at the "worst of the worst."

2) Investigate and identify the actual individual responsible for the infringing activities, not necessarily the subscriber.

3) Negotiate a settlement with the actual liable party, often declining offers from non-liable subscribers and when proper obtain an injunction or otherwise terminate the infringing activity. An injunction against a non-liable mere subscriber fails to address plaintiff's concerns.

4) Pursue, and if necessary litigate to trial with infringers with whom the termination of infringing activity and/or settlement cannot be reasonably obtained.

PLAINTIFF IS NOT 'MONETIZING' PIRACY

On scrutiny, the courts are finding that current enforcement practices used by counsel, are not to "plunder the citizenry," "exploit individuals," monetizing, or profiting from illegal downloading, but truly motivated by Plaintiff's desire to protect its copyrights interests and fight piracy.

As per the findings in similar cases:

> The action was not frivolous, was motivated by Dallas's desire to protect its copyright interests, and reasonably sought to recover compensation for, and deter future, copyright infringement. The relevant factors justify an award of attorney fees in this case. $10k judgment for damages; $6,708 for fees, and $892.00 in costs. *Dallas Buyers Club v. Vladamir Ivashentsev,* 3:15-cv-00220-AC, Ecf. 40 (D. OR. Feb. 11, 2016)

> The action was not frivolous, was motivated by Dallas's desire to protect its copyright interests, and reasonably sought to recover compensation for, and deter future, copyright infringement. Order Costs and Fees following $10k judgment. *Dallas Buyer Club v. Justin Klemmer*, 6:15-cv-00612-AC, Ecf. 33 (D. OR. Feb. 16, 2016)

And in accord with DBC's goals and the true purpose of legitimately addressing the root problem of piracy, DBC has often forgone the financial side of its enforcement program as evidenced in a number of settlements and consent judgments entered in its favor, including:

> In recognition of the financial hardship of DOE-98.232.132.220, with compliance with this Consent Judgment and Permanent Injunction plaintiff waives all claims for damages. *Dallas Buyers Club v. Doe-98.232.132.220,* 3:15-cv-00174-AC, Ecf. 16 (D. OR. May 20, 2015)

> In recognition of the financial hardship and extenuating circumstances in this case, plaintiff agrees that though the below Money Judgment shall be entered and enforceable, plaintiff will not execute or enforce the Money Judgment so long as the defendant complies with the below Permanent Injunction and is not involved with any future downloading, publishing or BitTorrent activity in violation of copyright law. *Dallas Buyers Club v. Krystal Krause*, 6:15-cv-00219-AC, Ecf. 16 (D. OR. May 22, 2015)

While the below Money Judgment is valid and fully enforceable, in recognition of the financial hardship of the defendant plaintiff agrees to not execute on the below Money Judgment so long as there is compliance with the terms of the settlement agreement and this Consent Judgment. *Dallas Buyers Club v. Ramon Fernandez,* 3:15-cv-00444-AC, Ecf. 34 (D. OR. Nov. 17, 2015)

In recognition of the financial hardship and extenuating circumstances in this case, plaintiff agrees that though the below Money Judgment shall be entered and enforceable, plaintiff will not execute or enforce the Money Judgment so long as the defendant complies with the parties Settlement Agreement and below Permanent Injunction and is not involved with any future downloading, publishing or BitTorrent activity in violation of copyright law. *Dallas Buyers Club v. Kent Deberry,* 6:15-cv-00611-AC, Ecf. 10 (D. OR. June 11, 2015)

In recognition of the financial hardship and extenuating circumstances in this case, plaintiff agrees that though the below Money Judgment shall be entered and enforceable, plaintiff will not execute or enforce the Money Judgment so long as the defendant complies with the below Permanent Injunction and is not involved with any future downloading, publishing or BitTorrent activity in violation of copyright law. *Dallas Buyers Club v. Victoria Ditkovsky,* 6:15-cv-00696-AC, ECF 13 (D. OR. July 24, 2015)

In recognition of the financial hardship of DOE-24.22.0.68, with compliance with this Consent Judgment and Permanent Injunction plaintiff waives all claims for damages. *Dallas Buyers Club v. Doe-24.22.0.68,* 3:15-cv-00729-AC, Ecf. 8 (D. OR. June 3, 2015)

> In consideration for the economic hardship of Doe 1103 I Doe-24.20.145.186, plaintiff waives all claims for damages. *Dallas Buyers Club v. Anonymous User of Popcorn Time*, 3:15-cv-01779-AC, Ecf. 11 (D. OR. Nov. 9, 2015)

The false narratives propounded by defense counsel and on the internet that "[t]he plaintiff's goal in these matters is not to reach a judgment on the merits, but rather to secure a dubious settlement in any amount…" is just an outright misstatement of the fact as demonstrated repeatedly in actual cases.

PLAINTIFF INVESTIGATION AND IDENTIFICATION ARE SUCCESSFUL

DBC has a demonstrated reliability in identifying actual infringers. The District Court of Oregon has found on examination: "Based on Plaintiffs' successful identification of defendants in the vast majority of the cases it has filed in 2014, the court finds it likely that the requested discovery will uncover the identity of the defendant in this case as well." *Voltage Pictures and Dallas Buyers Club v. Doe-50.141.97.4*, 3:14-cv-01872-AC, ECF 21 (April 9, 2015).

Plaintiff obtains this success in part by utilizing and scrutinizing data from multiple sources and by pursuing persistent infringers not merely the occasional downloader.

a. BitTorrent Operation

In general, BitTorrent operates with a number of parties joining in a swarm to both download files and share/upload files with other swarm members, commonly called peers. Members of a swarm broadcast, or register, their IP address with Trackers and Distributed Hash Tables ("DHT's") to allow them to be located and to locate other members sharing a distinct file. Both Trackers and DHT's are publicly broadcasted resources for anyone who wishes to locate and join a swarm to download a file. Files can be movies, T.V. shows, software, games or any available information being uploaded or distributed. In essence, Trackers and DHT's are lists of

IP addresses where uploaders/peers register as being a resource for others to download a specific file, or to find lists of others from whom they may download a file.

Plaintiff utilizes investigator MaverickEye, UG (http://www.maverickeye.de) for its pre-filing investigations. MaverickEye provides plaintiff with two primary resources. The first is a tool of general observed activity, called Cross-Reference Data or X-Ref Data. The second is a direct investigation of IP addresses that are observed uploading plaintiff's works called Capture Data. The investigative tools provided by MaverickEye are related but generate independent data and reflect distinct information. The two data sets are correlative only to the extent the two investigative tools might independently observe related events.

b. Cross-Reference (X-Ref) Data - Indirect Observations.

The Cross-Reference or "X-Ref" tool used by MaverickEye collects data from broadcast sources such as Trackers and DHT's. The data of the X-Ref tool reflects third party registrations of IP addresses as being a resource for anyone that wishes to join a swarm to download a file. Trackers and DHT's carry only limited registrations and are regularly updated. With hundreds of thousands of files being exchanged on BitTorrent at any one time, and millions of IP addresses trafficking in those files, the picture collected from Trackers and DHT's is a limited snapshot of files being trafficked at any one time. Any one Tracker or DHT's will not be a list of all files associated with any IP address any more than they will be a list of all IP addresses associated with any single file. Data collecting from Trackers and DHT's is commonly used in the industry for Digital Millennium Copyright Act (DMCA) notices and has been used as a basis for filing copyright infringement suits.

The X-Ref type of data, though valid, has a number of shortcomings.[2] While Trackers and DHT's are highly accurate, and this is the data that users of BitTorrent rely on to maintain the BitTorrent network, the data comes from unsecured third parties and only lists IP addresses that are registered as a resource for the distribution of files. There is no direct observation or bilateral confirmation of actual infringing activity. A second issue, if the registered IP address is reassigned between the time of registration and observation, the IP address might appear to belong to someone that has never infringed. Because of the shortcomings, plaintiff uses a second set of direct observation data as its basis for infringement complaints and uses the X-Ref indirect observation as secondary support evidence.

c. Capture Data – Direct Observations.

The primary data on which plaintiff relies in bringing its complaint is obtained through the Maverik Monitor ™ investigative tool. The Maverik Monitor tool independently obtains IP addresses that are trafficking in plaintiff's motion picture. The Maverik Monitor tool then joins the swarm as a peer to make a direct TCP/IP connection with other swarm participants. In doing so it makes a direct peer-to-peer connection with an infringing computer and downloads (but does not upload) a portion of the copyrighted material being shared.

In making this direct peer-to-peer connection, the Maverik Monitor tool confirms the defendant's IP address is actively broadcasting/distributing the file and not simply registered with a Tracker or DHT's as having the file available. It verifies the data downloaded as infringing data, and records the exact time of the direct peer-to-peer connection with the

[2] Paitek, M., Kohno, T., Krishnamurthy, A: Challenges and Directions for Monitoring P2P File Sharing Networks– or –Why My Printer Received a DMCA Takedown Notice. In Proceedings of the USENIX Workshop on Hot Topics in Security, San Jose, CA, USA (2008). Ref: http://dmca.cs.washington.edu/dmca_hotsec08.pdf

infringing computer. Concerns about reassigned IP addresses and the theoretical malicious "spoofing" of an IP address are overcome as the communications with the infringers' IP addresses are time-specific and bilateral, verified as being received and acknowledged by the infringer's computer. The Maverik Monitor tool is observing and documenting over 200 captures a day of the motion picture *Dallas Buyers Club.*

d. Value and Utility of X-Ref Data.

Plaintiff is only able to trace an IP address to a subscriber. Often a single household will have multiple occupants with access to the IP address. The broad data of the X-Ref tool continues to be very useful to both subscribers and plaintiff for identification purposes. X-Ref Data can confirm or eliminate the subscriber as the potential defendant, or provide a subscriber useful information on the types of shows, activities, or interests of the actual infringer and identify a pattern and practice of upload activity, narrowing the focus of any investigation of parties that may be actually infringing. In many cases, on review of the X-Ref Data the identity of the infringer or proper defendant becomes readily apparent. Moreover, this data is still the standard for many enforcement programs and has been found to be reliable evidence of infringing activity.

e. Old Technology and Isolated Cases Are Out of Context.

One of the most common arguments made by defendants and articulated by Judge Wright is an IP Address is insufficient to identify the infringer. *Ingenuity 13, LLC* at Pg. 4. This argument is supported by a number of older cases that base their investigation on older technology. The plaintiffs in these cases appear to have used X-Ref Data, the same as used for Digital Millennium Copyright Act (DMCA) notices. While courts have found this to be accurate and have issued warrants based on its use, Maverik Monitor investigative tool uses a more

advance method, by making a direct TCP/IP connection, similar to that being used by the FBI in fighting Child Porn. See United States v. Carter, 549 F. Supp. 2d 1257, 1260 (D. Nev. 2008) (Defendant actually connected to a covert FBI computer in San Jose, California. The FBI computer captured the Internet Protocol (IP) address).

More importantly, the Oregon District Court has monitored the accuracy of Plaintiffs' litigation and recognized the effectiveness of Plaintiffs' investigations in the "vast majority" of the cases filed. However, Plaintiffs' investigation will only get you to the right door or gateway. The information regarding who has access to the door or gateway is known to the subscriber. The Oregon District Court has determined after observations, trial and error, and working with counsel for both plaintiff and defense that an FRCP 45 deposition of the subscriber at the onset of a case is fair, effective, and cost efficient for all parties involved. Exhibits 1and 2.

MOTION FOR FRCP 45 DEPOSITION

Courts routinely allow discovery to identify "Doe" defendants operating through the Internet. See generally *Voltage, et. al v. Does:* 3:14-cv-01241-AC, (D. OR); *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980) ("where the identity of alleged defendants [are not] known prior to the filing of a complaint . . . the plaintiff should be given an opportunity through discovery to identify the unknown defendants"); *Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (error to dismiss unnamed defendants given possibility that identity could be ascertained through discovery). The issue that arises in these cases is not if early discovery will be allowed, but what is fair, effective, and cost efficient for all parties involved. In BitTorrent litigation there have been three methods used to determine the identity of an actual infringer after the subscriber has been identified by an ISP, Name the subscriber and proceed in the regular

course, request leave to seek FRCP 31 Deposition by Written Question, or depositions under FRCP 45.

In most cases, the location of the infringing activity is identified as the home or business of the subscriber. Plaintiff's data consists of specific times and dates in which The Maverik Monitor tool has made direct connections to a computer at the identified location. In these cases, defendants tend to raise one of a number of known, but factually implausible defenses such as the claim of dynamically assigned IPA's, Wi-Fi hacking, and the proverbial "ghost user" a/k/a the "it must have been a guest that stopped by" defense. Many courts, such as the U.S. District Court of Oregon, have realized these defenses are shams.

First, dynamically assigned IPA's are only an issue if the plaintiff does not know when the infringing activity occurred. Plaintiff's claim is not simply that an IPA was used to infringe, but that a specific IPA at a specific time was used to infringe and a direct connection was made to a computer at the location the IPA was assigned. Thus even if the IPA were assigned to a different party at a different time, it would not matter.

Second, in the thousands of civil cases filed, there are no known instances of Wi-Fi hacking. Plaintiff is not aware of any cases, where a subscriber has identified a hacker breaching the password protection of their internet service to seed or distribute movies. While it is surely possible, the technical skill, expensive equipment, time and significant effort to hack a modern Wi-Fi password are not likely to be expended for the use of BitTorrent by a neighbor.

Finally, Plaintiff's investigations have found that the subscriber is the actual infringer (as has generally been the case in over 60% of all cases filed) or in the vast majority of other cases, the subscriber knows the actual infringer (they have provided the access and the password) and is impeding plaintiff's investigation to protect the infringer as an accessory after the fact in a

ratification of the infringing activity. When ISPs install internet service to a location, that service is secured by a name and up to 16-digit password. This information would have to be provided to an individual by the subscriber for access to use the subscriber's internet service. Early access to the subscriber has been the key to identifying the infringing party in these cases.

1. NAMING THE SUBSCRIBER AND PROCEEDING IN THE REGULAR COURSE

In Judge Wright's order, he found with only the subscriber's subpoenaed IPA, a Plaintiff could only show that someone using that IPA was downloading. *Id*. at Pg. 6. Judge Wright was concerned that there was no further investigation to determine whether the subscriber actually downloaded the data or if someone else was using the subscriber's Internet access. Id. As per Judge Wright, and most courts, it is unreasonable to name a subscriber just because their IPA was identified as infringing. A proper investigation should seek to determine the actual infringer, not just the subscriber, and name the proper defendant. *Id.* The porno-trolls utilize fear tactics such as being stigmatized a social misfit or thief and being publicly associated with pornography as leverage to secure a settlement. Although plaintiff's motion pictures are not pornography, being identified as a thief can still lead to the same types of problems.

Moreover, under this method, discovery does not take place until after an answer has been filed and a rule 26 conference has taken place. After the deposition, if it is determined that the subscriber is not the infringing party, plaintiff is required to seek leave from the court to name and serve the identified party and start the process over again. This method causes delay, could lead to public shaming, increases the cost of litigation, increases motion practice and court time.

2. FRCP 31 DEPOSITION BY WRITTEN QUESTION

Plaintiff's counsel was guided to the use of FRCP 31 Deposition by Written question by Judge Elizabeth D. Laporte in response to a request for a FRCP 45 deposition of a subscriber. *Cobbler Nevada, LLC, v. Doe-73.15.228.64*, 3:15-cv-05313-EDL, Ecf. 24 (N.D. Cal. Feb. 24,

2016). Judge Laporte requested counsel suggest an alternative means of obtaining the needed information that was less burdensome than the requested 2-hour deposition and noted FRCP 31 Deposition by Written question. *Id.* Counsel for Plaintiff was currently filing cases in both the Northern and Southern District Court of California at the time and just days earlier had also received a denial of a request for FRCP 45 deposition of a subscriber in a Southern District case. *Dallas Buyers Club, LLC, v. Michael Ahmari,* 3:15-cv-01614-BAS-DHB, Ecf. 15 (S. D. Cal. Feb. 19, 2016). Plaintiff's counsel researched the suggest FRCP 31 Deposition by Written question and found that the leading case was a case from the Southern District of California. *See 808 Holdings LLC, v. Collective of Dec 29, 201, Sharing Hash 37917C8EEB4585E6421358FF32F29CD63C23C91*, 2012 WL 1648838, at *9 (S.D. Cal. May 4, 2012).

Based on the suggestion of Judge Laporte and research of the cases law from the Southern District, plaintiff's counsel requested leave to perform an FRCP 31 Deposition by Written Question. The proposed questions were submitted to the court and Judge Laporte modified the questions to be submitted to the subscriber. *Cobbler Nevada, LLC,* at 2. Counsel for the plaintiff continued to use the questions as modified by Judge Laporte in subsequent requests for FRCP 31 depositions in both the Northern and Southern Districts of California. Counsel included with all requests for FRCP 31 depositions, as an exhibit, the modified questions for the judge to review prior to submitting them to the subscriber. However, courts are reevaluating this method of discovery and finding it is not a "less intrusive alternative" to FRCP 45 depositions. *Dallas Buyers Club, LLC v. Doe-68.7.128.206,* 3:15-cv-00467-BAS-DHB, Ecf. 11 (S. D. Cal. July 15, 2016).

Courts have expressed two concerns regarding FRCP 31 Depositions by Written Question. First, it can be seen as "a procedure by which to propound interrogatories upon a non-party" which is contrary to the Federal Rules. *Cobbler Nevada, LLC, v. Doe-68.8.213.203,* 3:15-cv-02729-GPC-JMA, Ecf. 27 (July 5, 2016). In fact, Judge Alder, found the questions as modified by Judge Laporte, did "not comply with rule 31" and the subscriber "was under no

obligation to respond." *Id.* The difficulty in using this process is clearly shown. As a result of counsel for the Plaintiff using the questions as modified by Judge Laporte, Judge Bartick of the Southern District Court has stated counsel for Plaintiff has abused the process:

"In addition, the Court notes that Plaintiff's counsel has previously abused the procedure under Rule 31. *See Cobbler Nevada LLC v. Doe 68.8.213.203*, 15cv2729-GPC (JMA), ECF No. 27 (S.D. Cal. July 5, 2016) (denying motion to compel responses to deposition by written questions where counsel attempted to use Rule 31 in a manner that was functionally similar to interrogatories, which is improper and not permitted by the federal rules)." *Dallas Buyers Club, LLC v. Doe-68.7.128.206,* at 3.

This shows how difficult it is for a plaintiff to use this method to attempt to discover the identity of an infringer. There is no set of questions that will satisfy all parties, and the courts. In this case Federal judges have differing opinions as to what is considered abusive and should be allowed.

Secondly, as explained by Judge Bartick:

"Federal Rule of Civil Procedure 31 permits depositions of any person by written questions instead of by oral examination. Fed.R.Civ.P. 31(a). Based on the Rule's title, it may sound like a deposition by written questions is a less burdensome way to obtain deposition discovery. However, once the Rule is examined, it is clear that depositions by written questions "entail more than mailing questions to the deponents and awaiting their written response." *Dasenbrook v. Enenmoh,* 2015 WL 1889069, *2 (E.D. Cal. April 24, 2015). Rule 31 requires the party taking the deposition to deliver the written questions to a deposition officer. Fed.R.Civ.P. 31(b). The deposition then proceeds in a manner similar to oral depositions. *Id.* (incorporating Rule 30(c), (e), and (f)). The deponent is put under oath, and then the deposition officer "must ask the deponent [the written] questions and record the answers verbatim." Fed.R.Civ.P. 30(c)(3). Following the deposition, a transcript is prepared in the same manner as an oral deposition. Fed.R.Civ.P. 31(b)(2)-(3).

Therefore, Plaintiff's contention that a deposition by written questions is appropriate

here because it is a less intrusive alternative is without merit." *Dallas Buyers Club, LLC v. Doe-68.7.128.206,* at 3.

Finally, the use of written questions under FRCP 31 has been ineffective. The courts have limited the number of questions to 4. The results of the first 3 cases Plaintiff's counsel requested FRCP 31 depositions have led to 2 motions to compel and no response to the third. See *Cobbler Nevada, LLC, v. Sandra Bell,* 3:15-cv-05614, Ecf. 28 (N. D Cal. June 6, 2016), *Cobbler Nevada, LLC, v. Doe-68.8.213.203,* 3:15-cv-02729, Ecf. 19 (S.D. Cal. May, 6, 2016). Many subscribers will just not respond. When they do respond, the responses lead to the need for the request for additional discovery.

In all the cases filed the plaintiffs have two types of data that can span over many months. There are date and time of direct contact with the infringers computer at a specific location and the X-Ref data provides a profile of the infringer's identity. Being able to go over the times and date and types of content observed has been very useful in helping a subscriber identify the infringing party.

3. FRCP 45 DEPOSITIONS OF THE SUBSCRIBER

Limited FRCP 45 depositions of the subscriber have been determined to be fair, effective, and cost efficient for all parties involved. In an ideal world all subscribers who pay for internet service are law abiding citizens willing to cooperate in assisting plaintiffs to find out who was using their internet service to steal plaintiff's motion picture. Plaintiff can send polite letters, and often does send such letters, exemplars attached as Exhibits 3, 4. But we do not live in an idea world and often such letters are ignored.

As a first matter, based on limited experience, approximately 60% of the time it is the subscriber who is the infringer. Not surprisingly plaintiff's efforts to confirm that the subscriber is not a mere third party are thwarted by an infringer that has been advised, even by counsel, to ignore all communications short of compelled testimony. Thus compelled testimony is often required simply to confirm the subscriber is not an absent landlord or some other party that should not be further burdened.

On the limited occasions where a subscriber is not the liable party, it is then the likely reality that the persistent infringing activity is that of a roommate or relative and there is the understandable hesitation to voluntarily turn over someone with whom there is a close relationship. Absent the excuse of compelled testimony what else would a roommate be expected to do?

The reality is, in the minority of the cases when the subscriber is not the infringer, the subscriber is the person that has information that can identify an infringer. When ISPs generally install internet service to a location, that service is secured by a name and up to 16-digit password which was provided to an identifiable party to use the internet services, limiting the scope to a specific pool of possible defendants. With the actual dates of infringing activity and review of the X-Ref Data the identity of the infringer or proper defendant more often than not becomes readily apparent to all parties. A few exemplars of past validation of the X-Ref Data include:

- X-Ref Data including items from the rapper "2 Chains" and the Hip-Hop title "Kendrick Lamar ft. Drake – Poetic Justice" useful to affirm the subscriber, a male in his 60's, was unlikely to be the proper defendant in light of an adult son believed to live in the residence. Voltage Pictures and Dallas Buyers Club, LLC v. Doe-50.141.97.4, 3:14-cv-01872-AC, Dkt. 21 (D. Or. April 9, 2015).
- Dates of X-Ref data used to correspond with an employee schedule at the workplace to identify the specific employee infringer. Voltage Pictures and Dallas Buyers Club, LLC v. Doe-50.76.100.253, 3:14-cv-01242-AC, Dkt. 16 (D. Or. Oct. 6, 2014).
- The presence of specific university textbooks in X-Ref data useful in identifying the proper infringer among 20 fraternity occupants as the textbooks corresponded with specific classes. Voltage Pictures and Dallas Buyers Club, LLC v. Doe-98.232.236.10, 6:14-cv-01408-AC, Dkt. 12 (D. Or. Nov. 11, 2014).

Plaintiff has two independent sets of data that can assist in identifying the infringer. First, Plaintiff has Capture Data that show 77 captures of Plaintiff's motion pictures from 01/29/2016

to 03/13/2016. Second, Plaintiff has X-Ref data that contains 2316 other copyrighted works that the infringer is shown distributing from 03/03/2015 to 08/09/2016. Being able to review the dates and times of infringing activity and type of materials accessed by the infringing party, there is a high likelihood the subscriber can identifying the responsible party. This cannot be done with 4 questions as allowed by the court under FRCP 31 depositions. Moreover, the procedure under FRCP 45 would be less burdensome and be fair, effective, and cost efficient for all parties involved.

To the extent that the subscriber may perceive any burden, it should be noted that even if the subscriber did not personally infringe plaintiff's rights, most subscribers have already disregarded multiple notices of infringing activity issued pursuant to 17 USC 512(a). The subscribers are facilitating the infringing activity by providing internet service to the defendant, and many have allowed hundreds and possibly thousands of acts of infringement causing harm to plaintiffs and countless others.

4. Efforts to Date

To determine whether there is "good cause" to permit expedited discovery to identify doe defendants, courts commonly consider whether:

> (1) The plaintiff can identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court court; (2) the plaintiff has identified all previous steps taken to locate the elusive defendant; (3) the plaintiff's suit against defendant could withstand a motion to dismiss; and (4) the plaintiff has demonstrated that there is a reasonable likelihood of being able to identify the defendant through discovery such that service of process would be possible.

OpenMind Solutions, INc. v. Does 1-39, No. 11-3311, 2011 WL 4715200, at *2 (N.D. Cal. Oct. 7, 2011)(citing *Columbia Ins. Ci. V. seescandy.com*, 185 F.R.D. 578-80 (N.D. Cal. 1999)).

Plaintiff has met the "good cause" standard as evidenced by Plaintiff being granted early discovery. (Dkt. No. 7.) Subsequent to being granted early discovery, Plaintiff has undertaken the following specific additional steps: Plaintiff received a response for its subpoena from Comcast Cable on May 3, 2016 identifying: Bu Li, 5 Fratessa Ct., San Francisco, CA 94134, as the subscriber. Plaintiff sent out two letters one on May 3 and a second May 10, 2016. Plaintiff received a response from Mr. Li by mail on or about May 16, 2016. On June 8, 2016 Plaintiff

spoke to Mr. Li on the phone, Mr. Li. expressed his intent to help, by answering questions via email. On June 9, 2016, Plaintiff emailed Mr. Li questions. On June 10, 2016, Mr. Li responded to the email and again stated he would provide as much information as he could. Plaintiff has not heard from Mr. Li since the June 10th email and has called and sent follow up requests the last being July 26, 2016. Because Mr. Li has failed to respond, Plaintiff is requesting leave to perform an FRCP 45 deposition in Plaintiff's attempt to identify the infringing party.

CONCLUSION

Being able to review the dates and times of infringing activity and type of materials accessed by the infringing party, there is a high likelihood the subscriber can identifying the responsible party. Courts have not approved of naming a subscriber without investigation and actually identifying an infringer cannot be done with 4 questions as allowed by the court under FRCP 31 depositions. Deposition under FRCP 45 would be less burdensome, fair, effective, and cost efficient for all parties involved.

DATED: August 11, 2016.

/s/James S. Davis
James S. Davis CALBAR NO.207963
Jamesdee3080@msn.com
619-934-4600
Of attorneys for the plaintiff