E-FILED
Monday, 25 March, 2013 04:01:54 PM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
SPRINGFIELD DIVISION

MALIBU MEDIA, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No.: 12-cv-03211-SEM-BGC
	)	
PHAY LINTHAKHANH	)	
	)	
Defendant.	)	

DEFENDANT'S MOTION TO REQUIRE PLAINTIFF TO POST BOND FOR ATTORNEY FEES AND COSTS

NOW COMES Defendant, PHAY LINTHAKHANH, by and through his attorneys, and hereby moves this Honorable Court to require Plaintiff MALIBU MEDIA, LLC to post a bond for $62,000 to secure the ability to cover attorneys fees and costs that Defendant has and expects to incur in this action in the likely event Defendant prevails as a prevailing party under 17 U.S.C. § 505, Rule 11, and Rule 54 (d).

I. INTRODUCTION

Defendant Phay Linthakhanh ("Linthakhanh") has incurred costs and significant attorney fees in defending this meritless litigation and intends to seeks costs and attorney fees as a prevailing party under 17 U.S.C. § 505 and other authority, including but not limited to Rule 11 and Rule 54 (d). As described more fully below, Defendant meets the standards for the imposition of a security bond for costs and attorneys fees because Plaintiff is a foreign corporation, Defendant has a reasonable or better possibility of obtaining judgment in this action, and upon information and belief Plaintiff has no attachable assets within this court's jurisdiction.

Furthermore, investigation has revealed Plaintiff operates within nothing more than an apartment in Los Angeles. Therefore, unlike a case of a foreign manufacturer who

may have assets that are expensive and difficult to hide, making enforcement of a judgment is likely if inconvenient in a foreign jurisdiction, in this case it appears Plaintiff may have no more attachable assets than the cameras and linens it requires to produce its product. These circumstances present a heightened concern for collection from a foreign entity. A posting of a bond to assure Defendant's ability to collect its attorneys fees and costs is thus fair and appropriate.

Finally, Malibu Media cannot reasonably claim that hardship would result from posting a bond as it already has obtained settlements arising from a multitude of copyright infringement lawsuits in jurisdictions throughout the country 472 total, as of February 8, 2013, including at least 12 in the Central District of Illinois. (See Pacer Search 2-8-13, attached as Exhibit A).

II. ARGUMENT

The posting of a bond is a power of this court implied by the authority to award costs a prevailing party. Gay v. Chandra, 682 F.3d 590 at 594 (7th Cir. 2012), citing Anderson v. Steers, Sullivan, McNamar & Rogers, 998 F.2d 495, 496 (7th Cir.1993) (affirming dismissal). “[The] privilege to proceed without posting security for costs and fees is reserved to the many truly impoverished litigants who, within the District Court's sound discretion, would remain without legal remedy if such privilege were not afforded to them.” Brewster v. North American Van Lines, Inc., 461 F.2d 649 at 651 (7th Cir., 1972). The financial burden that Defendant, an ordinary citizen, is suffering from this meritless litigation by a prodigious litigant must be met with an equal assurance that he may recover his attorneys fees and costs as a prevailing party. A security bond is required by Illinois law to be imposed upon foreign entities as Plaintiff Malibu Media, and 7th Circuit precedent allows this court the authority to follow Illinois law and provide

Defendant with the financial assurance of being able to enforce a judgment for attorneys fees and costs against Plaintiff in a foreign jurisdiction.

A. LEGAL AUTHORITY TO IMPOSE A SECURITY BOND

District courts typically "follow the forum state's practice" when deciding whether security is appropriate. Simulnet E. Assocs. V. Ramada Hotel Operating Co., 37 F.3d 573, 574 (9th Cir. 1994). Turning to the Illinois Code of Civil Procedure, the State of Illinois requires security for costs before initiating an action where, as here, the Plaintiff is not a resident of the State. "Security for costs.... in all civil actions, where the plaintiff, or person for whose use an action is to be commenced, is not a resident of this State, the plaintiff, or person for whose use the action is to be commenced, shall, before he or she institutes such action, file, or cause to be filed, with the clerk of the court in which the action is to be commenced, security for costs" (735 ILCS 5/5-101). Section 5-104 allows security for costs if the court is satisfied that the Plaintiff is unable to pay the costs of the action, upon the motion of the Defendant, and if the Plaintiff does not pay the case can be dismissed. "[If] in any case the court is satisfied that any plaintiff is unable to pay the costs of the action, or that he or she is so unsettled as to endanger the officers of the court with respect to their legal claims, it shall be the duty of the court, on motion of the defendant or any officer of the court, to order the plaintiff, on or before a day in such order stated, to give security for the payment of costs in such action. If such plaintiff neglects or refuses, on or before the day in such order stated, to file a written instrument of some responsible person, being a resident of this state, whereby he or she shall bind himself or herself to pay all costs which have accrued, or may accrue in such action, the court shall, on motion, dismiss the action." (735 ILCS 5/5-104).

In *Gay v. Chandra*, the Seventh Circuit stated the purpose of a security bond was meant "to insure that whatever assets a party does possess will not have been dissipated or

otherwise have become unreachable by the time such costs actually are awarded." Gay v. Chandra, 682 F.3d 590, 594 – 95 (7th Cir. 2012), citing Selletti v. Carey, 173 F.3d 104, 112 (2d Cir.1999) (emphasis in original); see also In re Merrill Lynch Relocation Mgmt., Inc., 812 F.2d 1116, 1123 (9th Cir.1987) (rejecting constitutional challenge to rule allowing court to require non-resident parties to post cost bonds). This understanding of cost bonds has deep historical roots. The practice of requiring such bonds developed to help resident defendants collect costs when victorious against non-resident plaintiffs whose property was beyond the reach of the court. See John A. Gliedman, Access to Federal Courts and Security for Costs and Fees, 74 St. John's L.Rev. 953, 958–59 (2000). The practice was imported from English courts, which did not require that an impoverished party post security. Id. at 958."

The Seventh Circuit in *Gay* also cited with approval the First Circuit test which "instructs courts to weigh (1) the merits of the case, (2) the prejudice to the defendant of not requiring a bond, and (3) the prejudice to the plaintiff of requiring a bond." Id., citing Aggarwal v. Ponce School of Medicine, 745 F.2d 723, 727–28 (1st Cir.1984). The Seventh Circuit also looked to the Ninth and Second Circuits which follow the First Circuit's test regarding security for costs and decided it "agree[s] with the reasoning of these courts [and that it] is not inconsistent with [their] decision in Anderson, where [they] affirmed dismissal where the plaintiff had made no effort to show that he could not afford to post the required bond." *Gay* at 595. Several federal courts have enacted local rules regarding the imposition of a bond, or security for costs and fees.[1] Where there is no local rule regarding the imposition of security, courts have the authority to order the posting of a bond "when necessary to protect litigants and the judicial system." *Anderson v. Steers*,

[1] *See, e.g.,* N.D. Ill. LR65.3 (providing that, upon a showing of good cause, a court may impose a bond as security for payment of all filing fees, and "all costs of the action which the party filing it may be directed to pay to any other party");

Sullivan, McNamar & Rogers, 998 F.2d 495, 496 (7th Cir. 1993) (affirming the lower court's imposition of a $10,000 bond for fees and costs); *Sassower v. American Bar Ass'n*, 33 F.3d 733 (7th Cir. 1994) (imposing a $5,000 bond requirement on the plaintiff to cover "normal costs under Fed.R.Civ.P 54(d) and the potential for an award of sanctions under Fed.R.Civ.P. 11"). The purpose of a cost bond is to ensure that any assets possessed by the party will not have disappeared by the time costs are awarded. *Gay v. Chandra*, 682 F.3d 590, 594 (7th Cir. 2012) (*citing Selletti v. Carey*, 173 F.3d 104 (2d Cir. 1999)). Such bonds were originally devised "to help resident defendants collect costs when victorious against non-resident plaintiffs." *Id.* (*citing* John A. Gliedman, Access to Federal Courts and Security for Costs and Fees, 74 ST. JOHN'S L.REV. 953, 958-59 (2000)).

In cases in which attorney fees can be awarded pursuant to the underlying statute, such as this case arising under the Copyright Act, courts have included attorney fees and costs in the bond amount. *See Selletti v. Carey*, 173 F.R.D. 96, 101 (S.D.N.Y. 1997) (directing plaintiff to post a bond of $50,000 in light of the attorney fee provision in the Copyright Act); *see also Beverly Hills Design Studio (N.Y.) v. Morris*, 126 F.R.D. 33, 37 (S.D.N.Y. 1989) (noting that "[w]hen defendant is statutorily entitled to attorneys' fees, it is consistent that security may be required to cover them").

B. PLAINTIFF IS A FOREIGN ENTITY

Plaintiff, Malibu Media, is a non-resident California limited liability company located in a loft style "live-work" apartment located at 409 W. Olympic Blvd., Suite 501, Los Angeles, CA, 90015. *See*, Exhibit B; ¶6 Second Amended Complaint.

Upon information and belief, Plaintiff has no attachable assets within this court's jurisdiction.

C. <u>The Plaintiff is unlikely to prevail on the merits</u>

The first factor cited by *Gay* as to whether to require the posting of a bond is to weigh the merits of the case. In this case, plaintiff has failed to show any facts, as opposed to mere conclusions, as to its basis for accusing defendant of infringing its works (see infra, below). Defendant has explicitly denied downloading or sharing plaintiff's Works, or even possessing the BitTorrent protocol plaintiff avers was used in the infringing BitTorrent swarm (Exhibit. C Linthakhanh Affidavit ¶2,3,5), Furthermore, Defendant has denied that he as allowed any other person to download or share files using his Internet connection, and has denied having the BitTorrent protocol, or any other downloading protocol, on his computer. (Linthakhanh Affidavit ¶4). Without having BitTorrent on his computers, it was not possible for him to have committed any of the infringements alleged by Plaintiffs.

Indeed, federal courts across the country and the computer science literature (*see*, infra.) and have demonstrated the unreliability of plaintiff's methods of so-called identification of infringers. As the honorable Harold. A. Baker of this court has stated, "Where an IP address might actually identify an individual subscriber and address the correlation is still far from perfect, as illustrated in the MSNBC article. The infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment." VPR Internationale v. Does 1-1,017, No. 11-02068 (ECF Doc. 15 at 2), 2011 WL 8179128 (C.D. Ill. Apr. 29, 2011). Judge Baker was making clear that IP subscribers are not necessarily copyright infringers, and was referring to an MSNBC article by Carolyn Thompson of a raid by federal agents on a home that was linked to downloaded child pornography. "Agents eventually traced the downloads to a neighbor who had used multiple IP subscribers' Wi-Fi connections (including a secure connection from the State University of New York). *See* Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks* (April 25, 2011), http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless/." Id.

But the connection between an IP address and an ISP subscriber (and Defendant) is even more tenuous in BitTorrent copyright litigation than the problem wireless internet connections poses as illustrated in the child pornography raid above, **because too often the IP address has simply been faked ("framed") by the real infringer** - who can be located out of state or even out of the country from the ISP subscriber whose internet account is associated with the IP address at the time of the infringing BitTorrent swarm. In a nutshell, the problem is identity theft. Much like the person who wishes to get a job but has a criminal history and uses a fake social security number on its employment application, in BitTorrent swarms an IP address is often "made up" and the made-up IP address just happens to belong to somebody. There is a strong possibility that happened with Defendant Phay Linthakhanh's IP address.

This unacceptably high incidence of identity theft aka being framed (collecively "false Positives"), the mistaken connection of an IP address found within an infringing BitTorrent swarm to an innocent ISP subscriber, is a known problem yet Plaintiff continues to recklessly sue innocent defendants, including Phay Linthakhan here. This known problem of false positives make plaintiff's allegation that an IP address was registered to Defendant *not sufficient,* in and of itself, to support a claim that the individual is guilty of infringement. As Defendant stated in his affidavit that he did not even have Bit Torrent software, and Plaintiff alleges that BitTorrent software was in fact used, it appears more likely than not that Plaintiff will not prevail and that Defendant will be awarded his attorneys fees and costs, making a security bond appropriate.

1. Federal Courts Agree That An IP Address Does Not Identify the Infringer of Plaintiff's Copyright

Plaintiff's alleged basis for suing Defendant is a reference to a report (not included in its complaint) that "Defendant installed a BitTorrent client onto his or her computer" (¶12 Second Amended Complaint), and that "IPP extracted the resulting data emanating from the investigation, reviewed the evidence logs, and isolated the transactions and the IP address

associated therewith for the file identified by the SHA-l hash values set forth on Exhibit A (the "Unique Hash Numbers") (¶ 34 Second Amended Complaint). Defendant has denied using BitTorrent or infringing plaintiff's copyrighted materials.

Courts across the country have come to recognize that the "evidence" used by plaintiffs in BitTorrent cases are fraught with reliability problems. The court in *SBO Pictures* stated: "the ISP subscriber to whom a certain IP address was assigned may not be the same person who used the internet connection for illicit purposes." *SBO Pictures, Inc., supra*, 2011 WL 6002620, at *3. In other words, just because an IP address is registered to an individual does not mean that he or she is guilty of infringement when that IP address is used to commit infringing activity. Similarly, In re Bittorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, at *3 13 (E.D.N.Y. May 1, 2012), the district court explained that "it is no more likely that the subscriber to an IP address carried out a particular computer function ... than to say an individual who pays the telephone bill made a specific telephone call." The court explained that due to the increasing popularity of wireless routers, it is even more doubtful that the identity of the subscriber to an IP address correlates to the identity of infringer who used the address.

2. Plaintiff Fails To Show This Defendant Was The Infringer

Plaintiff has acted as recklessly by naming Phay Linthakhanh as the infringer based on its haphazard and incomplete investigation. Plaintiffs obtained Defendant Linthakhanh's identity and sued him because defendant was the listed subscriber for the Internet service account associated with an IP address during the period of time the same IP addresses was alleged to have been part of an infringing BitTorrent swarm. (**Second Amended Complaint ¶¶ 32-38**). Defendant has explicitly denied downloading or sharing plaintiff's Works, or even possessing the BitTorrent protocol plaintiff avers was used in the infringing BitTorrent swarm (Linthakhanh Affidavit ¶2,3,5), Furthermore, Defendant has denied that he as allowed any other person to download or share files using his Internet connection, and has denied having the BitTorrent

protocol, or any other downloading protocol, on his computer. (Linthakhanh Affidavit ¶4). Without having BitTorrent on his computers, it was not possible for him to have committed any of the infringements alleged by Plaintiffs. Plaintiff has not and cannot show that Defendant Phay Linthakhanh is the infringer instead of someone else, such as "other members of the household; family guests; or, the next door neighbor who may be leeching from the [defendant household's] Internet access. Thus, Plaintiff acted recklessly by naming [Defendant] as the infringer based on its haphazard and incomplete investigation." Exhibit E at 6, OSC Document 48 filed 02/07/13 in *Ingenuity 13 LLC v John Doe*, 2:12-cv-8333, Honorable Otis Wright presiding.

Just as with the Plaintiff in *Ingenuity 13*, here Plaintiff failed to find more than "an IP address, the name of the Bittorrent client used, the alleged time of download, and an unresponsive subscriber." Exhibit E at 6.

a. Plaintiff Fails To Show IPP's Methodology Controls for False Positives

The computer science literature has demonstrated since at least 2008 that BitTorrent monitoring has been plagued with "false positives" - that is, false associations of infringing activity with a particular IP address. For example, a recent article by the School of Computer Science, University of Birmingham, UK article[2] reaffirms the 2008 study by Piatek[3] et al. (see, *infra*) which showed that indirect monitoring was extensively used by enforcement agencies and that this study "demonstrated **the high rate of false positives** caused by this approach by **implicating innocent devices such as printers and wireless access points as file-sharers, which later received cease-and-desist letters**. More recent studies have confirmed that these flawed practices continue to be used."(Emphasis added).

[2] *The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent, www.cs.bham.ac.uk/~tpc/Papers/P2PMonitor.pdf accessed on March 11, 2013.*

[3] At the time of this article, Michael Piatek was completing his Ph.D. in computer science at the University of Washington, where he was advised by Tom Anderson and Arvind Krishnamurthy. His thesis work "focused on how to build Internet-scale services without relying on expensive, trusted infrastructure" and received the 2009 Google Ph.D. Fellowship in Computer Networking. *http://www.michaelpiatek.com//, accessed on March 11, 2013*.

In Piatek's 2008 study, "*Challenges and Directions for Monitoring P2P File Sharing Networks – or –Why My Printer Received a DMCA Takedown Notice*" coauthored by professors Tadayoshi Kohno and Arvind Krishnamurthy of the University of Washington's Department of Computer Science and Engineering, the authors found that **false positives (i.e. copyright enforcement methodologies incorrectly implicating IP addresses of being involved in an infringing BitTorrent swarm) are present for a multitude of reasons**. "Through extensive measurement of tens of thousands of BitTorrent swarms and analysis of hundreds of DMCA complaints, we have shown that a **malicious user can implicate arbitrary network endpoints in copyright infringement, and additional false positives may arise due to buggy software or timing effects**" (Emphases added). Exhibit D at 6, 7. These reasons include, but are not necessarily limited to:

a) A malicious user can implicate arbitrary IPs in illegal sharing today. Exhibit D at3

b) A malicious user can frame arbitrary IPs simply by naming his own misreporting tracker during the creation of the torrent and then uploading that torrent to

one of the many public aggregation websites that are crawled. Exhibit D at 3

c) IP addresses are leased and can be implicated to a new user after the actual infringer is done using the IP address ("Mistimed reports"). Exhibit D at 3, 4.

d) Anyone on the path between the tracker and a monitoring agent can alter the tracker's response, implicating arbitrary IP addresses ("Man in the Middle"). Exhibit D at 4.

e) Unbeknownst to the owner of the computer, the computer might be running malware that downloads or hosts copyrighted content, or their home network might have an open wireless access point that someone else uses to share copyrighted content. Exhibit D at 4.

As the authors summarize:

> **Practically any Internet user can be framed for copyright infringement today.** By profiling copyright enforcement in the popular BitTorrent file sharing system, we were able to generate hundreds of real DMCA takedown notices for computers at the University of Washington that never downloaded nor shared *any content whatsoever*. Further, we were able to remotely generate complaints for nonsense devices including several printers and a (non-NAT) wireless access point. Our results demonstrate several simple techniques that a malicious user could use to frame arbitrary network endpoints.
>
> **Even without being explicitly framed, innocent users may still receive complaints.** Because of the inconclusive techniques used to identify infringing BitTorrent users, users may receive DMCA complaints even if they have not been explicitly framed by a malicious user and even if they have *never* used P2P software!

http://dmca.cs.washington.edu/, accessed on March 11, 2013.

Thus, it has been known in the literature since at least 2008 (thus, five years) that there are serious problems with accusing even a particular IP address with online infringing activity. Yet, plaintiff provides absolutely no reasons for this court to believe that IPP, a company located outside the United States, has solved these methodological problems inherent with BitTorrent monitoring to demonstrate that when it puts forth an IP address as associated with an infringing BitTorrent swarm, that the association is vetted to be the ISP subscriber, rather than an IP address being faked.

4. Plaintiff Fails to Show the File was Viewable

In a BitTorrent copyright infringement case similarly flimsy as this one, the Central District of California federal court found plaintiff violated Rule 11(b)(3) for filing a pleading based on an IP snapshot as lacking factual foundation. Exhibit E, OSC in *Ingenuity 13 LLC v John Doe*, 2:12-cv-8333, Document 48 filed 02/07/13, Honorable Otis Wright presiding:

> To allege copyright infringement based on an IP snapshot is akin to alleging theft based on a single surveillance camera shot: a photo of a child reaching for candy from a display does not automatically mean he stole it. No Court would allow a lawsuit to be filed based on that amount of evidence. What is more, downloading data via the Bittorrent protocol is not like stealing candy. Stealing a piece of a chocolate bar, however small, is still theft; but copying an encrypted, unusable piece of a video file via the Bittorrent protocol may not be copyright infringement. In the former case, some chocolate was taken; in the latter case, an encrypted, unusable chunk

> of zeroes and ones. And as part of its prima facie copyright claim, Plaintiff must show that Defendants copied the copyrighted work. *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991). If a download was not completed, Plaintiff's lawsuit may be deemed frivolous.
>
> In this case, Plaintiff's reliance on snapshot evidence to establish its copyright infringement claims is misplaced. A reasonable investigation should include evidence showing that Defendants downloaded the entire copyrighted work—or at least a usable portion of a copyrighted work. Plaintiff has none of this—no evidence that Defendants completed their download, and no evidence that what they downloaded is a substantially similar copy of the copyrighted work. Thus, Plaintiff's attorney violated Rule 11(b)(3) for filing a pleading that lacks factual foundation.

Plaintiff failed to submit any *factual basis* such as a report or affidavit from any person at IPP authenticating proper steps were actually completed to verify the alleged files **were usable or viewable**, necessary to establish copyright infringement, rather than its a "snapshot" theory of evidence in its Second Amended Complaint; or why the actual infringer is the defendant when all it had was an IP address, the name of the Bittorrent client used, the alleged time of download, and an unresponsive subscriber.

In sum, plaintiff has failed to provide any facts as opposed to mere conclusions that the alleged file was viewable or usable, necessary to establish infringement claims.

D. <u>The Plaintiff Is Not Prejudiced By Having To Submit A Bond For Costs</u>

Courts are required to take the plaintiff's financial situation into account when imposing a bond requirement. *Gay v. Chandra*, 682 F.3d at 594. However, here, it cannot be reasonably said that Plaintiff Malibu Media has any grounds for avoiding a bond requirement due to lack of funds. Given the large number of lawsuits that Malibu Media has filed in the past year (and the settlement payments that can be inferred from the number of voluntary dismissals in those cases) it should have plenty of funds with which to post a bond. Here, Plaintiff Malibu Media is a limited liability company organized and existing under the laws of California, and has its

principal place of business in California. Therefore, this is an appropriate situation in which posting of a cost bond should be required.

E. Defendant Will Be Prejudiced If A Bond For Costs Is Not Imposed Because Plaintiff Is A Non-Resident

Posting of a bond for security is appropriate in situations where the plaintiff is domiciled outside of the forum jurisdiction, and does not have attachable assets within the jurisdiction. *See Beverly Hills Design Studio*, 126 F.R.D. at 36, 39 (S.D.N.Y. 1989) (imposing a $20,000 bond where plaintiff could not identify assets to satisfy a potential award of costs and fees, and noting that situations involving security bonds generally involve plaintiffs with no reachable assets). Furthermore, as Malibu Media is essentially operating out of an apartment in Los Angeles, its assets there may be no more than necessary to produce its works: cameras, sheets, and pillows. (See Exhibit B)

Given the large numbers of lawsuits brought by Malibu Media, and the expenses in association with each suit, is it extremely uncertain whether defendant Linthakhanh will be able to recover costs when he prevails in this action. Particularly given the questionable sufficiency of the plaintiffs' evidence, and Defendant's denial of even owning the BitTorrent software Plaintiff claims was used in the infringing activity it alleges, the likelihood that Malibu Media could find itself facing any number of orders for costs and fees, it is reasonable and necessary to order that Malibu Media post a bond for fees and costs in this case.

III. DEFENDANT'S EXPECTED COSTS

Defendant Linthakhanh has already incurred expenses in this lawsuit, and can reasonably expect to incur significantly more as the suit progresses. Section 505 of the Copyright Act provides that "the court may [. . .] award a reasonably attorney's fees to the prevailing party as part of the costs." 17 U.S.C. § 505. The district court must make the initial assessment of reasonable attorney fees based on a calculation of the lodestar. *See Johnson v. GDF Inc.*, 668

F.3d 927, 929 (7th Cir. 2012), *see also Kaylor-Trent v. Bonewicz*, No. 11-3332 (C.D. Ill. Jan. 9, 2013). The lodestar is the calculation of the hours reasonably expected multiplied by the reasonably hourly rate. *See Hensley v. Eckerhart*, 461 U.S. 424, 433 (1983); *Johnson*, at 929.

Plaintiff intends to take twenty to forty depositions and engage in extensive electronic discovery. Exhibit G at 2. Thus, defense counsel expects to expend at least 200 to 250 hours on this litigation, through summary judgment stage. Defense counsel's market rate of $250/hour is a reasonable hourly rate, as shown by evidence of charging and obtaining this rate in other litigation in similar jurisdictions, and by attached affidavit from local attorneys performing similar work. See, Exhibit F. Thus, a bond of at least $62,500 is reasonable and appropriate to be applied in this case.

A. Probable Length of Litigation

At this time, it is only possible to give a rough estimate of the expected number of hours that will be expended in this litigation. As stated above, an estimated calculation has been made by defense counsel, and given the complexity of a copyright infringement case and the twenty to forty depositions plaintiff has stated it intends to take, defense counsel can expect to expend between 200 to 250 hours on this litigation.

B. Reasonable Hourly Rate

The reasonable hourly rate must be determined in the context of the market rate in the geographic location. *See Pickett v. Sheridan Health Care Ctr.*, 664 F.3d 632, 640 (7th Cir. 2011). Where an attorney has an actual billing rate that he typically charges, then that rate is presumptively his hourly rate." *Id.* In the Seventh Circuit, "the best evidence of the market rate is the hourly rate the attorneys receive from paying clients for similar services." *Kaylor-Trent v. Bonewicz*, No. 11-3332 (C.D. Ill. Jan. 9, 2013) (*citing Mathur v. Board of Trustees of Southern Illinois University*, 317 F.3d 738, 743 (7th Cir. 2003)). Indeed, there is a preference in the Seventh Circuit to award attorneys the amount they would have earned from paying clients. *Id.*

Here, the actual rate charged by defense counsel in this case, and in other similar litigation is $250 an hour, which represents defense counsel's market rate. Additionally, defense counsel has attached an affidavit from Springfield attorney James Fahey attesting to an hourly rate of $260 per hour as reasonable for similar work in this district's geographic area.

Therefore, based upon an estimate of between 200 to 250 hours of legal work, at a reasonable hourly rate of $250/hour, Defendant Linthakhanh can expect to spend approximately $62,500. Additionally, defense counsel estimates that expected costs are in the range of $5,000 to $7,500 or more, depending on the expert witness fees and court reporter fees. Therefore, a bond amount of $62,500 is reasonable, and the Defendant requests that the court order Plaintiff to post a bond for anticipated fees and costs for $62,500

IV. CONCLUSION

In light of the foregoing, it is clear there is a reasonable chance or better that Defendant will prevail and Plaintiff Malibu Media will not be successful in its copyright infringement suit against Defendant Linthakhanh. Malibu Media's allegation of an IP address being involved in an infringing BitTorrent swarm is far from insufficient to prove that Linthakhanh is the infringer. Coupled with Linthakhanh's explicit denials of infringement and the established problem of IP addresses being faked, known as the false positive problem, leads to the conclusion that Linthakhanh has a reasonable probability of obtaining a judgment against Malibu Media, a foreign entity, including attorney fees and costs under the Copyright Act. Therefore, Defendant Linthakhanh respectfully requests this court to order Plaintiff Malibu Media, LLC, to post a bond in the amount of $62,500 for fees and costs.

Dated: March 25, 2013

Respectfully submitted,

By: /s/ Jeffrey J. Antonelli
Jeffrey J. Antonelli, Bar # 6271875

Attorney for Defendant
Antonelli Law, Ltd.
30 North LaSalle Street, Suite 3400
Chicago, IL 60602
Telephone: (312) 201-8310
Facsimile: (312) 332-4663
E-Mail: jeffrey@antonelli-law.com