## UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA FORT LAUDERDALE DIVISION

MALIBU MEDIA, LLC,	
Plaintiff,	) Civil Action Case No. <u>0:14-cv-61957-JIC</u>
v.	)
ROBERT DARE,	
Defendant.	)

# PLAINTIFF'S RESPONSES TO DEFENDANT'S FIRST SET OF INTERROGATORIES

Plaintiff, MALIBU MEDIA, LLC, responds to Defendant's First Set of Interrogatories served June 9, 2015, as follows:

## STATEMENT OF WILLINGNESS TO COOPERATE

Counsel for Plaintiff is prepared to discuss with counsel for Defendant the objections set forth below for the purpose of resolving any disputes that may arise over the responses to the interrogatories without the need for intervention by the Court.

# PLAINTIFF'S RESPONSES TO DEFENDANT'S FIRST SET OF INTERROGATORIES

1. Please identify each individual, excluding your attorneys, who prepared or assisted in the preparation of Plaintiff's responses to these Interrogatories.

Response to Interrogatory No. 1: Colette Field is the only person who answered these interrogatories. Mrs. Field is a Co-Owner of Plaintiff. Colette Field can be reached through Plaintiff's counsel of record.

2. For each and every denial made to Defendant's first Requests for Admissions, thoroughly explain the reason for the denial.

**Response to Interrogatory No. 2:** To the best of Plaintiff's knowledge, Defendant has not served his First Set of Requests for Admission. Accordingly, Plaintiff cannot respond to this request.

3. For each of the works, identify the exact date and time it was first uploaded onto x-art.com or xart.com and made available to the website's members and, for each, the individual who performed the upload?

Response to Interrogatory No. 3: See Exhibit B to Plaintiff's Complaint, wherein Plaintiff lists the dates of first publication for all copyrighted works at issue in this case. In their capacity as Co-Owners of Malibu Media, LLC, Brigham and Colette Field are responsible for maintaining, managing, and uploading the works on the website X-Art.com.

4. Have you made any attempts to determine exactly how your works got onto the Torrent streams in the first place, or who uploaded them there? If so, please detail and explain any and all such attempts.

Response to Interrogatory No. 4: The only way to identify the initial seeder is for an individual to either create the swarm or participate in the swarm very near the time of creation. Plaintiff, Excipio, and IPP did not seed the works nor were they participants during swarm creation. Therefore, Plaintiff cannot determine the identity of the initial seeder.

5. For each work, please identify each member who accessed that work on x-art.com or xart.com, from that work's "Date of First Publication' through the "Most Recent Hit" date, as those dates are indicated in Exhibit B to the Amended Complaint (Doc. 8-2), as well as the time and date of access.

Response to Interrogatory No. 5: This information does not exist. Regardless, Plaintiff objects to this interrogatory on the basis that it is harassing and seeks the disclosure of highly confidential trade secret information. Further it is not relevant. Indeed, Defendant would not depose the 50,000 subscribers nor subpoena and review their computers to ascertain the identification of the initial seeder. Further, the initial seeder may very well be in a foreign country. This interrogatory is the epitome of a bad faith discovery request. You have no intent or ability to use this information.

6. Have you ever found a member of xart.com or x-art.com to be sharing your copyrighted works on any peer-to-peer file-sharing site without authorization? If so, please identify the member, the work they were sharing, the date you identified them, and any demands made about the unauthorized sharing.

**Response to Interrogatory No. 6:** Plaintiff has never found a member of xart.com or x-art.com to be sharing its copyrighted works on any peer-to-peer file-sharing site without authorization.

7. Please list any and all dates and times at which IPP International UG "connected" with Defendant's IP address, as you allege in the Amended Complaint.

Response to Interrogatory No. 7: Pursuant to Fed. R. Civ. P. 33(d) since the answer to this interrogatory may be determined by examining the MySQL Log File and the burden of deriving or ascertaining this answer will be substantially the same for either party, the Plaintiff may answer by specifying the records that must be reviewed and giving the Defendant a reasonable opportunity to examine such records. Therefore, Plaintiff will produce a copy of the MySQL Log File which will list each date and time Defendant's IP Address connected to Excipio's servers and transmitted a piece of any of Plaintiff's copyrighted works at issue in this case.

8. Please list and identify any and all usernames, clientnames, pseudonyms, network names, globally unique identifier, port(s), and name of the protocol that IPP's software logged during the TCP/IP connection between IPP International UG and IP address 98.249.146.169, as referenced in the Amended Complaint.

**Response to Interrogatory No. 8:** Plaintiff will produce one PCAP for each work infringed and the MySQL log file. Plaintiff does not have any other information in its possession, custody, or control which is responsive to this request.

9. For each work, please identify, as best as possible, the initial file-provider. If said individual's name is unknown, provide the IP address, username, clientname, pseudonym, and/or network name, and whatever other identifying information you have.

**Response to Interrogatory No. 9:** Plaintiff does not know the identity of the initial seeder.

10. Please identify the exact date(s) and time(s) when the alleged downloads (a) began and (b) ended.

**Response to Interrogatory No. 10:** Plaintiff will produce the MySQL Log File which contains this information.

11. Please identify each and every user interacting, stating for each: (a) IP address; (b) user ID or other identifier; (c) legal name, address, and telephone number, if known; and (d) the dates and times of each said user interacting began and ended such activity.

**Response to Interrogatory No. 11:** Plaintiff does not have any information in its possession, custody, or control which is responsive to this request.

12. Regarding the torrent files, please identify: (a) the size of the file; (b) the number of "pieces" the file was broken into; (c) the size of each piece, and (c) the cryptographic "hash".

Response to Interrogatory No. 12: Pursuant to Fed. R. Civ. P. 33(d) since the answer to this interrogatory may be determined by examining the .torrent file and the burden of deriving or ascertaining this answer will be substantially the same for either party, the Plaintiff may answer by specifying the records that must be reviewed and giving the Defendant a reasonable opportunity to examine such records. Therefore, Plaintiff will produce a copy of each of the .torrent files which speak for themselves.

13. Did Defendant download the entire torrent files to completion? If your answer is "yes," please explain any and all facts on which you rely to arrive at that conclusion.

Response to Interrogatory No. 13: Yes. Obtaining a complete copy of a computer file is the purpose of using BitTorrent. And, Defendant obviously obtains complete files because he uses BitTorrent all of the time.

14. In publishing or producing the works that you allege Defendant infringed, were any devices, software, or mechanisms used to diminish infringing activity, such as copy protections, anti-piracy software protection, or piracy protection? If so, describe them in detail.

Response to Interrogatory No. 14: Yes. But these measures are not relevant or likely to lead to the discovery of admissible evidence. Plaintiff did not authorize Defendant to steal seventeen of its works.

AMENDED Response to Interrogatory No. 14: Yes. Plaintiff hires skilled programmers and a data security firm to secure its website from hackers or others who aim to breach Plaintiff's website security and illegally access Plaintiff's videos through its website. Additionally, Plaintiff has an employee who methodologically polices online infringing websites and employs a strategy through DMCA notices to reduce piracy of its content. By way of example, in the month of August, Plaintiff's DMCA notice employee sent 62,992 DMCA notices to stop Plaintiff's infringing content on the Internet. These notices were sent to remove files, images, videos, posts, and search engine links either containing or directing individuals to Plaintiff's illegally infringed content. This effort resulted in the successful takedown of 4,857 videos.

Additionally, Plaintiff's website (legal page) states: "Copyright The content, materials, images, designs and other media (collectively, the "Content") which appear on x-art.com are protected by United States and worldwide copyright laws and may not be reproduced,

transmitted, copied, edited, or published in any way whatsoever without the written permission of x-art.com. Unauthorized reproduction, distribution or use of the Content is strictly prohibited. Without exception, copyright violators will be pursued and prosecuted to the fullest extent of the law." Further, Plaintiff obtained copyright registrations for all of its works. And, Plaintiff files suit and litigates against the most egregious infringers of its content to deter them, and others like them, from illegally downloading and distributing Plaintiff's works on the Internet.

15. What actions have you taken to diminish piracy of the works? Please be as specific and detailed as possible.

**Response to Interrogatory No. 15:** See Response to Interrogatory No. 14.

AMENDED Response to Interrogatory No. 15: Yes. Plaintiff hires skilled programmers and a data security firm to secure its website from hackers or others who aim to breach Plaintiff's website security and illegally access Plaintiff's videos through its website. Additionally, Plaintiff has an employee who methodologically polices online infringing websites and employs a strategy through DMCA notices to reduce piracy of its content. By way of example, in the month of August, Plaintiff's DMCA notice employee sent 62,992 DMCA notices to stop Plaintiff's infringing content on the Internet. These notices were sent to remove files, images, videos, posts, and search engine links either containing or directing individuals to Plaintiff's illegally infringed content. This effort resulted in the successful takedown of 4,857 videos.

Additionally, Plaintiff's website (legal page) states: "Copyright The content, materials, images, designs and other media (collectively, the "Content") which appear on x-art.com are protected by United States and worldwide copyright laws and may not be reproduced,

transmitted, copied, edited, or published in any way whatsoever without the written permission of x-art.com. Unauthorized reproduction, distribution or use of the Content is strictly prohibited. Without exception, copyright violators will be pursued and prosecuted to the fullest extent of the law." Further, Plaintiff obtained copyright registrations for all of its works. And, Plaintiff files suit and litigates against the most egregious infringers of its content to deter them, and others like them, from illegally downloading and distributing Plaintiff's works on the Internet.

16. For each and every work, please identify by address the filming location, the date(s) of filming, and whether a film permit was issued for filming, and if so, the agency issuing the permit.

Response to Interrogatory No. 16: Plaintiff objects on the basis that this request seeks information that is neither relevant nor likely to lead to the discovery of admissible information. Plaintiff further objects on the basis that this request is set forth solely to harass Plaintiff.

17. For each and every work, please specify whether, during filming, a condom or dental dam was used in every instance of oral sex and every instance of sexual penetration.

Response to Interrogatory No. 17: Plaintiff objects on the basis that this request seeks information that is neither relevant nor likely to lead to the discovery of admissible information. Plaintiff objects on the basis that this request seeks confidential business information. Plaintiff further objects on the basis that this request is set forth solely to harass Plaintiff. Further, none of these answers would affect the copyright ability of the works.

18. Do you have any evidence, other than an IP Address, to prove that Defendant, ROBERT DARE, and no one else committed the infringements alleged in the amended complaint? If so, please identify, with particularity and to completion, any and all such evidence.

Response to Interrogatory No. 18: Plaintiff objects on the basis that this interrogatory seeks attorney mental impressions. Further, it is premature to explain evidence because discovery is ongoing. Plaintiff's evidence will be explained in dispositive motions and at trial, if necessary.

AMENDED Response to Interrogatory No. 18: Plaintiff objects on the basis that this interrogatory seeks attorney mental impressions. Further, it is premature to explain evidence because discovery is ongoing. Plaintiff's evidence will be explained in dispositive motions and at trial, if necessary. Plaintiff reserves the right to supplement this interrogatory as discovery in ongoing and it is continually discovering new information that demonstrates Defendant is the infringer. Toward that end, Plaintiff does not know at this time which evidence it will use or produce for trial.

Notwithstanding the foregoing, Plaintiff's response is as follows:

Plaintiff discovered that an individual using Defendant's IP address infringed seventeen (17) of its copyrighted works between March 15, 2014 and June 8, 2014. Plaintiff's investigator, IPP, established a direct TCP/IP connection with the Defendant's IP address. IPP downloaded from Defendant one or more bits of each of the infringing digital movie files. Further, IPP possesses the recording of this infringement in the form of PCAPs, which Plaintiff has already produced to Defendant. These PCAPs irrefutably prove that the infringement occurred from Defendant's IP address. Because Plaintiff considers Defendant to be a *serial* infringer of its

copyrighted works, Plaintiff's investigators monitored and obtained additional evidence of Defendant's BitTorrent activity and cross-referenced Defendant's IP address to its database, the results of which form Plaintiff's "Additional Evidence" In doing so, Plaintiff has learned that Defendant's IP address has continually infringed third-party copyrighted works such as mainstream movies and television shows. Indeed, Defendant infringed three hundred and fifteen (315) third-party works between July 2013 and December 2014.

Discovery revealed Defendant's employment history as a Java Developer, Senior Java Developer, Senior Software Engineer, Senior Software Architect, Development Manager, and Chief Cloud Architect. In total, Defendant used his sophisticated technological experience to build: (1) back-end server components in Java, including data base design and user interface; (2) the Motorola iFUN System; (3) an international payment and shipping system; (4) various telecommunication and OSS products that were resold to companies like Cisco, SBC (now AT&T), and T-Mobile; (5) a cloud based advertisement network and lead generation exchange platform; and (6) a Cloud Platform for handling big data and Bluetooth Low-Energy device management software.

Defendant also claimed that he purchased a Netgear N600 Wireless Dual Band Router in June 2013, which was password protected between June 2013 until February 2014. Notably, Plaintiff's Additional Evidence shows Defendant infringing third-party copyrighted works every single month between July 2013 through December 9, 2013 – a period in time during which Defendant claims his internet was password protected.

Additionally, Defendant claims that between December 2013 and February 2014, he deactivated his cable modem due to an extended family trip abroad. Plaintiff's Additional

<sup>[1]</sup> Plaintiff titles this the "Additional Evidence" and produced it to Defendant.

evidence demonstrates that between December 9, 2013 and February 17, 2014, all infringement stopped.

Defendant stated, under oath, that in February 2014, he removed his internet password to accommodate guests, and that he secured his internet after receiving notice of this lawsuit from Comcast. Comcast's subpoena notice went out in October, 2014. Plaintiff's Additional evidence demonstrates Defendant's IP address *continued* to infringe third-party works after he received the Comcast Notice. In fact, Defendant's infringements continued until December 8, 2014 – the exact date in which Plaintiff' amended its Complaint to proceed against Defendant.

Plaintiff's investigators were also able to determine that infringement of Plaintiff's works were accomplished through use of "Transmission 2.42" - a BitTorrent client specifically made for use on a Mac computer. As Plaintiff anticipated, discovery revealed that Defendant only possessed and used one computer in his home during the period of recorded infringement – a MacBook Pro. Defendant claimed that he obtained the MacBook Pro from his prior employer, OpenPeak, which he subsequently returned once his employment ended in August 2014. This correlates with the infringement dates on the Additional Evidence.

19. Explain, in as much detail as possible, in chronological order with dates, each and every step used by your investigator to detect the transmission of the works through Defendant's IP address.

Response to Interrogatory No. 19: Plaintiff does not have sufficient information in its possession, custody or control to answer this interrogatory. Excipio recorded the infringement. Therefore, this request should be directed to Excipio.

#### **AMENDED Response to Interrogatory No. 19:**

As far as Plaintiff understands and is aware, Plaintiff's investigator detected the transmission of the works through the following process:

The data collection system used by IPP has the following components:

- a. a proprietary BitTorrent Client;
- b. a proprietary program analyzing the BitTorrent traffic and writes infringing transactions to a database;
- c. servers running a MySQL database cluster which log verified infringing transactions;
- d. packet analyzers, also known as packet sniffers, which create and analyze PCAPs;
- e. servers that run the proprietary BitTorrent Client, the BitTorrent analyzer and record PCAPs;
- f. WORM ("Write Once Read Many") tape drives for storing the PCAPs, the torrent data and MySQL server data;
- g. a program to synchronize the servers' clocks with both a GPS clock and an atom clock;
- h. a proprietary program for checking the MySQL log files against the contents of the PCAPs; and
- i. a proprietary program which checks the information contained in an Excel Spreadsheet against what is in the PCAPs and server's log files.

Excipio's data collection system accurately collected and recorded evidence proving that the defendant infringed Plaintiff's copyrighted work(s). The dates in which Excipio's data collection system collected and recorded evidence that Defendant infringed Plaintiff's works are set forth on the MySQL log and Additional Evidence which Plaintiff has provided Defendant.

The first step in the evidence collection process is for the Plaintiff, here Malibu Media, LLC, to provide Excipio with the titles of the copyrighted content. This is done by IPP on an ongoing basis on or around the dates when Plaintiff's movies are published. Excipio then conducts a lexical search for the titles on well-known torrent websites. Torrent websites host torrent files. To download content through BitTorrent a user will first download a BitTorrent client (software that enables the BitTorrent protocol work), and then search for torrent files on torrent websites. The BitTorrent client is then used to download the torrent file from the website.

When Excipio's lexical search yields matches, Excipio downloads the torrent files and joins the swarms of BitTorrent peers distributing a computer file – here, copies of Plaintiff's copyrighted movie(s). The peers in a BitTorrent swarm connect to each other's computers in order to transmit "pieces" of the computer file. Every "piece" of the computer file – and the entire computer file – transmitted via BitTorrent has its own unique hash value. A hash value is a digital fingerprint for a piece of data.

Excipio uses a proprietary BitTorrent client to connect to the swarm of infringers unlawfully sharing Plaintiff's copyrighted movies. Once Excipio has joined the swarm, its system begins logging the infringing transactions with BitTorrent peers. The software <u>does not</u> upload or distribute content; it was created such that it is incapable of doing so.

Excipio's system connects to the infringing peers using a TCP/IP connection. This connection cannot be spoofed. Once the connection is established, the system begins the process of downloading a piece or pieces of the infringing computer file from the computer connected to the internet through the Defendant's IP address. The entire process and all of the transactions are recorded and stored in Excipio's database.

Data sent through the internet is delivered in the form of "packets" of information.

PCAP stands for "Packet Capture." A PCAP is a computer file containing captured or recorded data transmitted between two computers. A "Packet Analyzer" records packets of data being transmitted between two computers over a network, such as the internet, and saves it in a PCAP. Packet analyzers also enable users to read and analyze PCAPs. PCAPs are akin to videotapes, but instead of recording light and sound they record zeroes and ones.

Excipio's data collection system uses a proprietary packet analyzer and TCPDump (a free open-source packet analyzer) to record the infringing transactions in PCAPs. Both of these were in good working order at the time the PCAP was captured and recorded.

TCPDump is widely used and is capable of accurately recording network traffic flowing to and from a computer in the form of PCAPs.

Here, the PCAPs are recordings of numerous BitTorrent computer transactions during which a person using Defendant's IP Address sent pieces of an infringing computer file (which contain an unlawful copy of Plaintiff's works) to Excipio's servers. Michael Patzer personally maintains and monitors the servers.

Each PCAP clearly shows the IP address distributing the BitTorrent piece (Defendant's IP address), the IP address receiving the BitTorrent piece (Excipio's IP address), what was transmitted (a piece of Malibu Media's copyrighted movie(s)), the transaction protocol (*i.e.* BitTorrent), and the time of the infringing transaction.

Each infringing transaction is also recorded on a MySQL server log file. *See* Excel Containing MySQL data. Each entry on the MySQL log file correlates to a specific PCAP file in Excipio's possession. The MySQL log file was created by a MySQL database which I installed and which was in good working order at the time the data was logged. The PCAPs and MySQL server log files are saved onto WORM tape drives. WORM stands for "write once read many".

Excipio uses these because it is impossible to modify or delete the data after it has been written to a WORM tape drive. Indeed, the WORM tape drive is not capable of being manipulated or altered. And, the only way to destroy the data is to destroy the WORM tape drive itself. Each of the WORM tape drives is electronically stamped with a German government issued time stamp at least every twenty four hours. The drives are then stored in a computer safe for safekeeping.

When the PCAP and MySQL log file evidence is provided to a party, the WORM tape drive on which the evidence was written and stored is located and the data then digitally restored. If asked, Michael Patzer could and would bring the actual computer files to trial in this matter. Only 1 PCAP per movie infringed is produced to the Plaintiff usually. 1 PCAP per movie is sufficient to prove without question that the infringement of each of the movies at issue occurred. Producing <u>all</u> PCAPs for each of the infringed movies would be superfluous and extremely time consuming.

In addition to producing 1 PCAP per movie and the MySQL server log file, Plaintiff's investigators also produce the following:

j. One (1) Technical Report per movie. The Technical Reports are included merely for ease of reference and only translate the electronic data contained in the PCAPs to an easy to understand format. The first part of the Technical Report lists *all* of the infringing transactions committed by someone using Defendant's IP address for the specific movie. Each line correlates to a line of the MySQL log file. As previously stated, Excipio has a PCAP for each entry on the MySQL log file. The second part of the Technical Report pertains to the specific PCAP that was produced for that movie. The relevant lines from the PCAP are reproduced and explained in the Technical Report. Because PCAPs actually contain hundreds of

different fields, reproducing only the relevant lines of the PCAP in the Technical Report makes the PCAP easier to understand. Highlighting the relevant lines in no way changes what the PCAP says but instead, merely points to the relevant information in the computer file which shows that someone using Defendant's IP address sent a piece of Plaintiff's copyrighted work to Excipio's servers.

- k. One .tar file for each work infringed. The .tar files contain the actual media files Defendant's IP address was distributing (i.e. the unlawful copy of Plaintiff's movie).
- One .torrent file for each work infringed. The .torrent file is the computer file
  which allows the BitTorrent user's BitTorrent client to locate tracker computers
  within the peer-to-peer network and connect to the swarm.

A distributed hash table (DHT) is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures. BitTorrent clients use a "Distributed Hash Table" (DHT) to locate peers who are downloading a torrent file. Specifically, a BitTorrent client locates and connects to the DHT. After the DHT locates peers, it requests the IP address for each peer. Using this process BitTorrent users are able to locate and connect to a number of peers within a particular swarm.

Excipio's infringement detection system uses servers which are programmed to crawl popular torrent websites. In the process, the servers locate third party torrent files. The servers

subsequently download the torrent files from these websites. Similar to BitTorrent clients, Excipio's system uses a DHT to obtain the IP Addresses of peers registered to each torrent file. Excipio's system uses nodes to locate peers downloading a specific torrent-file. After locating the peers, Excipio's system requests a list of all the registered peers within the swarm. All responses are saved in a database. This includes the IP addresses, dates, hash values, and file names corresponding to the torrent-files. The results of a search within the database for Defendant's IP address are attached hereto as Exhibit "B." The database records show Defendant's IP address was a registered peer within the swarms for each of the third party works listed on at the dates provided on Plaintiff's Additional Evidence.

20. Did you ever send an investigator to Defendant's physical location, or nearby it, to investigate Defendant or Defendant's internet connection on location? If so, please identify said investigator(s), describe the investigation method(s), and state the dates and times of these investigations.

Response to Interrogatory No. 20: Plaintiff has not yet sent an investigator to or nearby Defendant's physical location to investigate Defendant or Defendant's internet connection on location.

21. List each item of expense, loss, or damage you have incurred as a result of the incident sued on in this action, giving for each: the date incurred, the name and address of the person, firm, or entity to whom owed or paid, and the goods or services for which each sum was incurred.

Response to Interrogatory No. 21: Plaintiff only seeks to recover statutory damages. Therefore, Plaintiff objects to this request on the basis that it seeks information that is neither relevant nor likely to lead to the discovery of admissible information. Nevertheless, Plaintiff avers it has suffered substantial actual damages from BitTorrent copyright infringement. The basis for determining the quantum of these damages would be a reasonable royalty for the worldwide distribution of Plaintiff's copyrighted works over the internet. Plaintiff would not enter into a license with a third party which authorizes such distribution for less than the statutory maximum award under the Copyright Act. The exact dollar amount that BitTorrent infringement costs Plaintiff in lost sales is uncertain and requires assumptions to be made about the number of infringers who would become subscribers but for the availability of BitTorrent. Over 80,000 unique individuals infringe Malibu Media's works in the U.S. each month alone. If Plaintiff had 80,000 new subscribers per month, its revenue would increase by ten figures. Plaintiff has zero doubt that BitTorrent infringement costs it several million dollars in lost profits every year.

22. Please identify each user interacting and any and all settlement(s) or recovery received from, and all judgments entered against, each and every such user listed.

Response to Interrogatory No. 22: Plaintiff does not possess a list of "each user interacting" and therefore cannot respond to this request.

#### **DECLARATION**

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 4<sup>th</sup> day of September, 2015.

#### **COLETTE PELISSIER FIELD**

Dated: July 13, 2015

Date Amended: September 4, 2015

Respectfully submitted,

By: /s/ M. Keith Lipscomb
M. Keith Lipscomb (429554)
klipscomb@lebfirm.com
LIPSCOMB EISENBERG & BAKER, PL
2 South Biscayne Blvd.
Penthouse 3800
Miami, FL 33131
Telephone: (786) 431-2228
Facsimile: (786) 431-2229

## **CERTIFICATE OF SERVICE**

I hereby certify that on September 4, 2015, I electronically mailed the foregoing document to Cynthia Conlin at cynthia@cynthiaconlin.com.

By: /s/ M. Keith Lipscomb

Attorneys for Plaintiff

### Case 0:14-cv-61957-JIC Document 73-8 Entered on FLSD Docket 10/20/2015 Page 20 of 20

PURSUANT TO 28 U .S.C. § 1746, I hereby declare under penalty of perjury under the

laws of the United States of America that the foregoing is true and correct.

Executed on this 4th day of September, 2015.

COLETTE PELISSIER FIELD

By: Calette Felin

Dated: July 13, 2015

Date Amended: September 4, 2015

Respectfully submitted,

By: /s/ M. Keith Lipscomb

M. Keith Lipscomb (429554)
klipscomb@lebfirm.com
LIPSCOMB EISENBERG & BAKER, PL
2 South Biscayne Blvd.
Penthouse 3800
Miami, FL 33131
Telephone: (786) 431-2228
Facsimile: (786) 431-2229

## CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2015, I electronically mailed the foregoing document to Cynthia Conlin at cynthia@cynthiaconlin.com.

By: /s/ M. Keith Lipscomb

Attorneys for Plaintiff