IN THE CIRCUIT COURT OF THE 17th
JUDICIAL CIRCUIT IN AND FOR
BROWARD COUNTY, FLORIDA

CASE NO. 12-034123 (07)

P & S ASSOCIATES GENERAL
PARTNERSHIP, etc. et al.,

Plaintiffs,
v.

STEVEN JACOB, et al.

Defendants.
_____/

PLAINTIFFS' NOTICE OF FILING DECLARATION OF JASON PARK IN SUPPORT OF SECOND RENEWED MOTION FOR TURNOVER OF COMPUTERS

Plaintiffs, by and through undersigned counsel, hereby give notice of filing the Declaration of Jason Park in Support of Plaintiffs' Second Renewed Motion to Compel Defendants Frank Avellino and Michael Bienes to Produce Computers for Inspection and to Produce Documents. The Declaration is attached hereto as **Exhibit A.**

Respectfully submitted,

BERGER SINGERMAN LLP
Attorneys for Plaintiffs
350 East Las Olas Blvd, Suite 1000
Fort Lauderdale, FL 33301
Telephone: (954) 525-9900
Facsimile: (954) 523-2872

By: */s/ Leonard K. Samuels*
Leonard K. Samuels
Florida Bar No. 501610
lsamuels@bergersingerman.com
Michel O. Weisz
Florida Bar No. 336939
mweisz@bergersingerman.com
Zachary P. Hyman
Florida Bar No. 98581
zhyman@bergersingerman.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on June 24, 2016, a copy of the foregoing was filed with the Clerk of the Court via the E-filing Portal, and served via Electronic Mail by the E-filing Portal upon:

Peter G. Herman, Esq.
The Herman Law Group, P.A.
1401 E. Broward Blvd., Suite 206
Fort Lauderdale, FL 33301
Tel.: 954-525-7500
Fax.: 954-761-8475
pgh@thglaw.com

Attorneys for Steven Jacob; Steven F. Jacob CPA & Associates, Inc.

Thomas M. Messana, Esq.
Messana, P.A.
401 East Las Olas Boulevard, Suite 1400
Fort Lauderdale, FL 33301
Tel.: 954-712-7400
Fax: 954-712-7401
tmessana@messana-law.com

Attorneys for Plaintiff

Gary A. Woodfield, Esq.
Haile, Shaw & Pfaffenberger, P.A.
660 U.S. Highway One, Third Floor
North Palm Beach, FL 33408
Tel.: 561-627-8100
Fax.: 561-622-7603
gwoodfiled@haileshaw.com
bpetroni@haileshaw.com
eservices@haileshaw.com

Attorneys for Frank Avellino and Michael Bienes

By: *s/Leonard K. Samuels*
Leonard K. Samuels

EXHIBIT A

IN THE CIRCUIT COURT OF THE 17th
JUDICIAL CIRCUIT IN AND FOR
BROWARD COUNTY, FLORIDA

CASE NO. 12-034123 (07)

P & S ASSOCIATES GENERAL
PARTNERSHIP, etc. et al.,

Plaintiffs,

vs.

STEVEN JACOB, et al.

Defendants.
_____/

DECLARATION OF JASON PARK IN SUPPORT OF SECOND RENEWED MOTION FOR TURNOVER OF COMPUTERS

I, Jason Park, pursuant to Pursuant to Fla. Stat. § 95.525(2), states as follows:

1. I am over eighteen (18) years of age and competent to testify to the matters stated herein.

2. I am Director of Forensic Services for US Legal Support, a litigation services firm located at 1580 Lincoln Street, Suite 930, Denver, Colorado 80203. Prior to working at US Legal Support, I was a Computer Forensic Examiner and Trainer at MD5 Group, LLC. In my capacity as a Forensic Examiner and Trainer, I have spent 8 years educating people as to how to conduct a forensic analysis of a computer.

3. In addition to the foregoing, I have more than 12 years of experience conducting forensic analysis of computers and 22 years of experience in automated litigation support. I have conducted a forensic analysis of hundreds of different computers, servers and phones.

4. Based on my experience, examining a user's e-mail account remotely through a web browser, or downloading the current contents of an email account is an ineffective means of locating e-mails or other documents which were accessed by the owner of the e-mail account, especially where there are issues concerning the possible deletion of e-mails. If a user accesses his e-mail through an actual computer program ("Email Client"), the Email Client may save e-mails on his hard disk, in an email database or in a separate folder. Accordingly, even if the e-mail is deleted from the email provider's database, those e-mails may still recovered through a forensic examination of that user's computer, and they may still be on the hard drive on that computer.

5. On the other hand, if a user used a web browser to access his e-mail, various files or fragments of files can automatically be saved on that user's computer. Those files may contain e-mails or other documents which were viewed via the user's web browser. Those files can be recovered, and the fragments can be reconstructed through a forensic analysis of a computer.

6. Certain portions of webpages, copies of webpages, and other information accessed through a user's web browser is often saved on a computer's hard drive. When a user accesses a web browser, the contents of what they view may be cached on the user's hard drive. Although files in a computer's cache may be overwritten, fragments of those files are often preserved. Accordingly, the fragments may be used to reconstruct the data.

7. Like files in the cache, files which are processed through a computer's Random Access Memory ("RAM") may be saved to the computer's hard drive. (RAM is the type of memory which allows a computer to run programs). The contents of the RAM may be written to the hard drive in a location named "pagefile.sys". Documents may be recovered from the pagefile.sys.

8. Any documents which are opened or downloaded through the Internet or via an e-mail client are automatically saved on a computer. Those files and their locations on a hard drive are generally not known by an average computer user, and therefore may not have been deleted.

9. Thus, attachments to e-mails, which were opened are likely to be present on a computer's hard drive, unless the user has located and intentionally deleted them.

10. Even if documents were deleted, those documents may be recovered. When a user deletes a file in the ordinary use of a computer, the file remains on the hard drive until the space that file occupies is overwritten by new data. Absent a high level of sophistication with computers or purposeful use of specialized software to ensure permanent deletion by overwriting the deleted file, the ordinary deletion of a file does not completely remove it from a computer. Instead, a deleted file is overwritten by another one.

11. Simply put, absent specialized expertise in computer systems or use of file wiping tools, an ordinary user will not be able to purposely overwrite files from a computer in a way that would render them unrecoverable. However, it is possible for portions of the unallocated (free) space to be overwritten by the operating system itself during the regular course of operation.

12. Further, information concerning the frequency with which a user accesses their e-mail can be determined through a forensic analysis of their computers. Computers regularly save information concerning when a user accesses a particular website. Thus, if a user did not access their e-mail during a particular period of time via a web browser, that is something that may be determined.

13. Accordingly, if there are none of the artifacts described above, it may be indicate that a computer user has intentionally deleted files, because the many of the files and folders are automatically preserved, unless a party seeks to delete them.

14. Because computer forensics involves an analysis of the data concerning a particular file or document, and not necessarily the actual contents of such a file, a forensic examiner can reconstruct deleted or otherwise overwritten files and data without viewing the underlying document itself. Simply put, a forensic analysis can be designed in such a way that viewing the actual contents of files can be avoided.

15. There are additional safeguards to protect a user's privacy when conducting a forensic analysis of a computer. It's possible to provide an index of files or fragments of files to a user before attempting to view of export them. Additionally, entering into confidentiality and/or non-disclosure agreements is very common when it comes to a forensic analysis of computers.

16. All of these processes can also be completed with minimum intrusion to a particular user, through the creation of a "forensic image" of a computer hard drive. A forensic image is a bit by bit clone of the data held on the drive and which creates an exact replica of the original hard drive, including metadata, stored on a hard drive. The forensic image is made while utilizing "write blocking" techniques. Write blocking prevents any data from the original hard drive from being altered.

Verification Pursuant to Fla. Stat. § 95.525(2)

Under penalties of perjury, I declare that I have read the foregoing Declaration and that the facts stated in it are true.

Dated June 24, 2016

JASON PARK