UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

JABIL INC.,

Plaintiff,

v.

ESSENTIUM, INC.; ESSENTIUM MATERIALS, LLC; ERIK GJOVIK; GREG OJEDA; WILLIAM "TERRY" MACNEISH III; and LARS UFFHAUSEN,

Defendants.

Case No. 8:19-cv-1567-T-23SPF

DECLARATION OF MARK LANTERMAN

Under 28 U.S.C. § 1746, I declare as follows:

1. My name is Mark Lanterman. I am the Chief Technology Officer of Computer Forensic Services ("CFS") located in Minnetonka, Minnesota. CFS and I have been retained by Greenberg Traurig, PA, to analyze digital evidence in this action.

2. Our firm specializes in the analysis of digital evidence in civil and criminal litigation. I have over 25 years of experience in computer forensics and cybersecurity. Prior to joining CFS, I was a sworn investigator for the United States Secret Service Electronic Crimes Task Force and acted as its senior computer forensic analyst.

3. I am certified by the United States Department of Homeland Security as a "Seized Computer Evidence Recovery Specialist," as well as certified in computer forensics by the National White-Collar Crime Center. Both federal and state court judges have appointed me as a neutral computer forensic analyst and special master.

4. I graduated from Upsala College in New Jersey with both a Bachelor of Science and a Master's degree in computer science. I completed post graduate work in cyber security at Harvard University.

5. I am currently adjunct faculty of computer science for the University of Minnesota Technological Leadership Institute's Master of Science and Security Technologies program (MSST). I am also faculty at the Mitchell Hamline School of Law and a professor of cybersecurity at the University of St. Thomas School of Law in Minnesota. I am also faculty for the National Judicial College in Reno, Nevada and the Federal Judicial Center in Washington D.C.

6. I have previously provided training or delivered keynote addresses for the United States Supreme Court; the Eleventh Circuit Federal Judicial Conference; the Eighth Circuit Federal Judicial Conference; the Southern District of Georgia; the Western District of Tennessee; and several state judicial conferences. I recently delivered the keynote address at the Chief Justices' Conference in Newport, Rhode Island. In 2018, I delivered the keynote address at Georgetown Law School's e-discovery conference.

7. I was appointed by the Minnesota Supreme Court to serve as a member of Minnesota's Lawyers' Professional Responsibility Board (LPRB). I was recently appointed to sit on its Opinion Committee.

8. I am a co-author of the Minnesota State Bar's e-Discovery Deskbook, and I also write monthly articles for *Minnesota Bench & Bar* magazine.

9. CFS is the exclusive, contracted computer forensic expert for the Hennepin County Sheriff's Office; the Ramsey County Attorney's Office; the Washington County

Attorney's Office in Minnesota; as well as the Metropolitan Airports Commission, also known as the Minneapolis/Saint Paul International Airport. CFS is also partnered with the U.S. Secret Service to assist with its electronic investigations.

10. CFS and I were engaged by Greenberg Traurig on October 21, 2019, to assist with the analysis of digital evidence in the above-captioned lawsuit. I offer this Declaration to discuss the preliminary results of my analysis of digital evidence provided to me to date. Because the results are preliminary, I reserve the right to supplement this Declaration after I am able to devote additional time to the digital evidence I have already received, and as additional information becomes available.

11. I am familiar with the facts as alleged, and Plaintiff's counsel has provided me with the pleadings, and Defendants' Motion to Compel and for Protective Order ("Defendants' Motion") filed on October 23, 2019.

12. Additionally, counsel has provided me with relevant "log" data. I understand that Jabil uses data-loss-prevention software called Digital Guardian. Among other functions, Digital Guardian helps Jabil to identify malicious programs and malicious user actions (including data copying) by tracking and logging file activity on Jabil computers. I understand that, at the direction of Greenberg Traurig, Jabil used Digital Guardian to generate logs of file activities associated with multiple employee numbers, including those of Defendants Terry MacNeish and Erik Gjovik ("the logs").[1] Counsel provided copies of these logs to me for analysis on October 31, 2019.

[1] Each Jabil employee is assigned a unique employee number, so that activities may be more easily tracked and identified in resulting log files.

13. In addition to contextual documents and the logs, Plaintiff's counsel has also provided "forensic images" of two Jabil-owned computers.[2] I understand that these forensic images represent computers that were used by Defendants during their tenure with Jabil. Forensic "imaging" is a process used to create a copy of an electronic device's data, including deleted data. The comprehensive nature of this preservation process allows for the assembly of a timeline of user actions. More specifically, the process preserves data such as logs, deleted data, and Internet browsing records, which in the aggregate create a narrative of user actions.

14. In summary, consistent with the opinions expressed in this Declaration, and based upon the materials that have been made available to me, I have concluded thus far that there is evidence to support the following:

a. Using a workstation computer located at a Jabil facility where Defendants MacNeish, Gjovik, and Ojeda formerly worked ("the workstation"), a user profile associated with Defendant MacNeish was used to "package" relevant Computer Aided Design ("CAD") and other files that appear to represent Jabil intellectual property on September 13, 2017;

b. On September 13, 2017, the workstation was used to export a list of Jabil contacts to a file called "Jabil Contacts1.CSV;"

c. On September 13, 2017, shortly after the files were packaged and the "contacts" file was created, a USB data storage device was attached to the workstation;

[2] CFS was provided with a forensic image designated as "Q-19-DT-178357-Kiosk" on October 30, 2019. CFS later received a forensic image designated as "Q-19-DT-178355-2nd_Floor_workstation" on November 4, 2019.

d. The logs contain evidence that another laptop assigned to Defendant MacNeish by Jabil was used to interact with "cloud" services on December 7, 2017—months after his resignation.[3] According to the logs, the cloud service data repository contained CAD and other files that are the same or similar to the files that were "packaged" on September 13, 2017.

15. For the purposes of this Declaration, all dates/times are reported in the time zone in which the workstation was set—Pacific Standard Time.

16. As noted above, one of the forensic images that I have started to analyze represents a workstation computer that was located at a Jabil facility where Defendants MacNeish, Gjovik, and Ojeda formerly worked.[4] I determined that by June 20, 2017, the workstation was put into service. At that time, the workstation's "Registered Owner" was designated as "Terry," and a user profile called "terry" was created.

17. Later, on July 7, 2017, another user profile called "100031794" was created. I understand that this number is Defendant MacNeish's Jabil employee identification number. (*See supra* fn. 1.)

18. I further understand that Defendant MacNeish resigned from Jabil on September 13, and left the company on September 15, 2017. (*See* Defendants' Motion at 3; Compl. ¶ 36.)

[3] "Cloud" accounts, generally, are used to centrally store files so that they can be accessed remotely from any computer or device connected to the Internet.

[4] The forensic image is named "Q-19-DT-178357-Kiosk", and was created on September 23, 2019.

19. On September 12, 2017, the "100031794" profile was used to package files into a compressed archive called "Terry Local Desktop ZIP - 9-12-2017.zip."[5] Notably, this file was stored in "OneDrive." OneDrive is a "cloud" file storage service offered by Microsoft. (*See supra* fn. 3.) Thus, the OneDrive account, to which the file was uploaded, afforded anyone with knowledge of the OneDrive account's username as password the capability of accessing and downloading the file from any computer that can access the Internet.

20. On September 13, 2017, the date of Defendant MacNeish's resignation and two days before his last day of employment at Jabil, a user logged into the workstation using Defendant MacNeish's employee number profile. During the morning of September 13, 2017 (approximately 7:35 AM), that user searched the Internet for "outlook export collected email addresses," using the Firefox web browser. Shortly thereafter (approximately 7:40 AM), I have identified indications that the user using Defendant MacNeish's employee number profile indeed exported a list of contacts, saving them to a file located at: "\Users\100031794\Desktop\Jabil Contacts1.CSV." To date, I have not recovered the content of this file from the forensic image of the workstation, but the evidence indicates that the file may have included the fields: name, address, Billing Information, Categories, Importance, Mileage, and Sensitivity.

21. Later in the morning of September 13, 2017, the same user then created another ZIP archive file called simply "jabil.zip." The "jabil.zip" file contained thousands of CAD and other files, a large majority of which were stored within subfolders, including

[5] A ZIP file (a file with a .zip file extension) is, essentially, a container that allows for the compression and packaging of several files. ZIP files are often used to facilitate file transfers to another device.

"FDM\CAD\10X Machine." I am familiar with the allegations underlying this action and understand "FDM" to mean fused deposition modeling (also known as fused filament fabrication), "CAD" to refer to Computer-Aided Design, and "10X" to refer to Jabil's TenX 3D-printing platform. (*See,* generally, Compl.)

22. The "jabil.zip" file was created on September 13, 2017, at approximately 9:42 AM. The file was last modified that same day at approximately 9:48 AM. This is consistent with the time it would have taken to "package" the CAD and other files into the ZIP container.

23. Minutes after the "jabil.zip" container completed the packaging process, at approximately 9:52 AM, a USB data storage device was attached to workstation, while it was logged into using Defendant MacNeish's employee number profile.

24. I also note that on August 25, 2017, a user, while logged into the workstation using Defendant MacNeish's profile, conducted a search on the Internet for "ccleaner." CCleaner is a commercially and freely available data wiping/cleanup software tool. While the program was installed, and set to run when the computer started up, I have not determined the extent, if any, of its usage.

25. CFS and I understand from Jabil that Defendant MacNeish was also issued a laptop that was owned by Jabil and intended for use in connection with MacNeish's job responsibilities (the "laptop"). I understand further that the laptop is not in Jabil's possession. However, the Digital Guardian logs indicate that the laptop was accessed (powered on, and connected to the Internet) after Defendant MacNeish's resignation from Jabil, using a profile associated with his employee identification number.

26. For example, the logs show that on December 7, 2017, Defendant MacNeish's profile was used to access the laptop, and the laptop synchronized with, and downloaded files from, a Dropbox account. Dropbox is a cloud data-storage service that offers the ability to upload and access files from multiple devices. According to the logs, when the laptop synchronized with Dropbox on December 7, 2017, thousands of CAD and other files were downloaded from the Dropbox account.

27. Notably, the files, as they existed in Dropbox, were contained within a folder called "Jabil." A substantial amount of the files had been stored in subfolders including: "fdm/cad/10x machine." This is the same folder path that I observed in the "jabil.zip" file created at Jabil using Defendant MacNeish's profile less than three months earlier.

28. The logs also show that Defendant MacNeish's profile continued to be used to access the laptop well into 2018. CFS and I understand that Greenberg Traurig has requested that the Defendants immediately return the laptop, but Defendants have thus far failed to do so. I have requested that Plaintiff's counsel provide that laptop to me for forensic preservation and analysis.

29. CFS and I are also in the process of reviewing Digital Guardian logs of activity associated with Defendant Erik Gjovik's employee number.

30. CFS's investigation and forensic analysis is ongoing. Indeed, I received the forensic images less than one week prior to the execution of this Declaration. For this reason, I respectfully reserve the right, to amend and supplement this Declaration.

I declare under penalty of perjury under the law of the United States that the foregoing is true and correct.

Executed on November 6, 2019

Mark Lanterman