IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

INTERNATIONAL FINANCIAL COMPANY, LLC,	:	**CIVIL ACTION**
Plaintiff,	:	
	:	
v.	:	
	:	**NO. 18-cv-2120**
ODARA JABALI-JETER,	:	
Defendant.	:	

MEMORANDUM

LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE **May 28, 2019**

Presently before the Court is Plaintiff International Financial Company, LLC's Motion for Sanctions and Contempt (ECF No. 18), and Defendant's Response in Opposition. (ECF No. 20). By Order dated August 15, 2018, the Honorable C. Darnell Jones II referred this matter to me. (Order, ECF No. 19). For the following reasons, Plaintiff's Motion for Sanctions will be GRANTED. Further, as set forth more fully below, and pursuant to 28 U.S.C. § 636(e)(6)(B), this Court certifies the facts setting out a prima facie case of Civil Contempt, and orders Defendant Odara Jabali-Jeter to appear before the Honorable C. Darnell Jones II for a hearing to show cause why she should not be held in contempt.

I. PROCEDURAL HISTORY

On May 21, 2018, Plaintiff International Financial Company, LLC ("IFC" or "Plaintiff") filed its Complaint seeking money damages and injunctive relief against its former employee, Defendant Odara Jabali-Jeter, ("Defendant"), alleging misappropriation of trade secrets, breach of contract, unfair competition, and other related counts. (Compl., ECF No. 1). Plaintiff, a real estate management company, avers that while Defendant was employed at IFC, she downloaded

confidential and proprietary information from Plaintiff's server onto personal flash drives, which she then transferred onto her personal computer, and subsequently utilized that information in her own real estate management company, which she was operating in competition with Plaintiff. (*Id.* at ¶¶ 11-16).

Also on May 21, 2018, Plaintiff filed a Motion for Temporary Restraining Order. (Mot. Temp. Restraining Order, ECF No. 3). Following a show cause hearing held on May 23, 2018, (ECF Nos. 5, 9), the Honorable C. Darnell Jones II issued a Temporary Restraining Order. (Order, ECF No. 10). Judge Jones ordered Defendant to, *inter alia*, deliver to Plaintiff all its documents and information no later than June 6, 2018, and take steps to preserve and prevent the automatic or intentional deletion of all databases, electronic files, or computer hard drives. (*Id.*). On June 6, 2018, pursuant to Judge Jones' Order, Defendant delivered to Plaintiff a single USB drive containing eleven files and tendered her personal laptop for forensic examination.

On August 14, 2018, Plaintiff filed a Motion for Sanctions and Contempt against Defendant, asserting that she had willfully destroyed evidence unfavorable to her, in violation of the Judges Jones' May 29, 2018 Temporary Restraining Order. (Pl.'s Mot. Sanctions & Contempt, ECF No. 18). Plaintiff previously hired a forensic expert who examined Defendant's work laptop, and opined that Defendant had plugged in at least six flash drives to download information from her work computer. (*Id.* at 3-6). Plaintiff's forensic expert, Mr. Ashraf Massoud, also examined Defendant's personal laptop, and Plaintiff asserts "despite establishing the presence of Plaintiff's Information on these flash drives, and despite establishing that Defendant had connected these flash drives to both the Defendant's personal and work laptops, Mr. Massoud could not find *any* files identified in his prior Affidavit on Defendant's personal

laptop." (*Id.* at 13; *see also* Pl.'s Mot. for Temporary Restraining Order, ECF No. 3, Ex. A, Aff. of Ashraf Massoud).

By Order dated August 15, 2018, Judge Jones referred Plaintiff's Motion for Sanctions and Contempt to me. (Order, ECF No. 19). On September 13, 2018, the Court held an evidentiary hearing on Plaintiff's Motion. (ECF Nos. 22, 26). Defendant testified at the hearing, as did IFC's Executive Vice President, Mr. Victor Rodin, and IFC's forensic expert, Mr. Ashraf Massoud. (Tr., ECF No. 30). The parties submitted their Proposed Findings of Fact and Conclusions of Law. (ECF Nos. 28, 32).

The Court has reviewed the testimony and the parties' Proposed Findings of Fact and Conclusions of Law, as well as the exhibits introduced at the evidentiary hearing. Upon this record, the Court makes the following findings.

II. FINDINGS OF FACT

To briefly summarize, Defendant worked as Director of Operations, Management, and Events for IFC as one of three full time employees—along with its President, Mr. Neal Rodin, and Executive Vice President, Mr. Victor Rodin. As Operations Director, Defendant handled IFC's confidential business information, as well as tenants' confidential information. In August 2017, the Rodins discovered various deleted data entries from IFC's secure electronic server, and noticed some physical files were missing from IFC's locked office space. The Rodins conducted an investigation and hired a forensic IT consultant to examine Defendant's work-issued laptop, and discovered Defendant had downloaded IFC's confidential business information onto multiple flash drives. The IT consultant discovered that Defendant had been operating her own real estate management company, in competition with Plaintiff. Consequently, IFC terminated

Defendant's employment, and requested Defendant to return its confidential and proprietary information. Defendant has failed to return IFC's property.

Defendant initially denied that she downloaded IFC's confidential information onto flash drives. She subsequently admitted she downloaded IFC's information, but stated that she lost the flash drives. Pursuant to the Court's Temporary Restraining Order entered on May 29, 2018, she produced one flash drive containing eleven documents. She additionally produced her personal laptop for forensic examination. Forensic examination of Defendant's personal laptop revealed that Defendant had additional IFC information which she had not produced, as required by the Court's Temporary Restraining Order. Further, the forensic examination of her personal laptop revealed evidence of tampering.

First, I will describe the parties and provide my findings of fact as to the background of the instant litigation. Second, I will describe the results of the forensic examination of Defendant's work laptop; specifically, the evidence of Defendant's USB drive usage and downloading IFC's information onto those USB drives. Next, I will summarize Defendant's termination from IFC and her subsequent communications and administrative charges against IFC. Then, I will describe the Court's May 29, 2018 Temporary Restraining Order ("TRO") and Defendant's June 6, 2018 production of a USB drive and her personal laptop pursuant to the TRO. Lastly, I will provide my factual findings regarding the forensic examination of Defendant's personal laptop, focusing on the evidence of tampering and evidence of IFC's property which Defendant failed to produce as required by the Court's Order.

A. The Parties

1. Plaintiff International Financial Company, LLC, is a limited liability corporation with its principal place of business located at 1617 John F. Kennedy Boulevard, Suite 1840, Philadelphia, Pennsylvania, 19103. (Pl.'s Compl., at ¶ 4).

2. IFC is a real estate management company and is owned and operated by the Rodin family. IFC's President, Neal Rodin, founded the company in the 1990's. (Pl.'s Proposed Findings of Fact & Conclusions of Law, ECF No. 32, at ¶ 3). Neal Rodin's son, Victor Rodin, has worked at IFC since late 2011, and is its executive vice president. (*Id.* at ¶ 4; Tr., ECF No. 30, at 127:24-128:17).

3. Defendant Odara Jabali-Jeter is an adult individual and former employee of IFC. She presently resides in Philadelphia, Pennsylvania. (*Id.* at ¶ 5; Def.'s Proposed Findings of Fact & Conclusions of Law, ECF No. 28, at ¶ 2; *see also* Tr., ECF No. 30, at 7:5-10).

B. Overview of the Parties' Relationship

4. Defendant began working as a part-time employee doing bookkeeping at IFC in 2008 and became a full-time employee in 2010. (Tr., at 9:8-10:23). When she became a full-time employee, she was the "Director of Operations, Management and Events," and was one of IFC's three full-time employees, along with Neal and Victor Rodin. (*Id.* at 132:2-16). Defendant's job duties as Director of Operations, Management and Events included, *inter alia*, "maintaining and updating IFC's business files such as rent rolls, profit and loss statements for real estate properties, customer contact lists, customer turnover logs, lease amendment logs, repair schedules, reviewing property services invoices, banking and transaction logs, generating event schedule, taking notes during business transaction and meetings, and communicating with customers and other individuals as necessary to perform [her] work for IFC." (*Id.* at 11:7-15).

5. Defendant also managed various properties for IFC, as well as its books, escrow accounts, and personnel files. (*Id.* at 11:17-12:9; *see also e.g.*, Pl.'s Ex. 39). As the office manager, she received confidential information such as tenant's social security numbers, bank numbers and records, and rent checks. (Tr., at 11:22-15:17, 132:9-16). Defendant recognized and testified that when she "received the confidential information, [she] had a duty to preserve it." (*Id.* at 15:15-17). Indeed, Defendant admitted that, as IFC's office manager, she "was the one that went around and made sure that people signed the confidentiality agreement." (*Id.* at 130:23-24). For example, when Victor Rodin began working at IFC in 2011, Defendant presented the confidentiality agreement to him for signature, and signed as the witness. (*Id.* at 130:1-19; *see also* Pl.'s Ex. 36 (Victor Rodin Confidentiality Agreement)).

6. IFC issued laptops to its full-time employees (Defendant, Victor Rodin, and Neal Rodin) for work purposes, and each laptop had "[their] own username and [their] own password." (*Id.* at 133:14-15). For example, Defendant's username was "Odara" and no one else knew her password. (*Id.* at 133:10-134:6). The work laptops interfaced into the "Rodin Server" which IFC used for its confidential information and business records. (*Id.* at 134:7-18).

7. Victor Rodin testified that IFC never permitted Defendant to download or transfer files onto flash drives to take home for work purposes, because "[t]hat's why we have work laptops." (*Id.* at 138:20-25). He further testified that, although it was rare, he and Defendant would occasionally "bring our work laptops home if we needed them for say a

vacation or something else. I mean, it was rare, but there's no reason for her to copy the information [onto flash drives] because she could have just brought her laptop with her." (*Id.* at 139:1-5).

C. Background of the Instant Litigation: August and September 2017

8. Towards the end of August 2017, the Rodins were out of IFC's office: Neal Rodin was out of town and Victor Rodin was preparing to go on vacation. (*Id.* at 139:19-21, 140:21-23). While preparing to go on vacation, Victor Rodin examined IFC's company calendar on the software program Microsoft Outlook. (*Id.* at 140:7-141:19). Victor Rodin, Neal Rodin, and Defendant utilized IFC's Outlook calendar to log both "personal stuff, if we needed to take a couple of hours for doctor's appointments or anything personal, it didn't really matter, we would put that in the calendar along with professional meetings that we had." (*Id.* at 140:7-11). However, as Defendant and Victor Rodin testified, only Defendant and Victor Rodin made entries to, or altered, the Outlook calendar. (*Id.* at 36:19-24; 141:12-15).

9. Victor Rodin discovered "a lot of deletions of calendar events" which were specifically related to Defendant's personal events. (*Id.* at 140:12-23). He testified that he "didn't see a single evidence in our calendar of where Odara had asked for time and we gave her, which we always gave her time." (*Id.* at 140:15-17). Victor Rodin informed Neal Rodin that Defendant's personal entries had been deleted from the Outlook calendar, and Victor Rodin did not delete them. (*Id.* at 140:20-25; 141:16-25).

10. Victor Rodin and Neal Rodin initially did not think that Defendant had deleted the entries. (*Id.* at 141:25-142:3). Victor Rodin stated that he and his father decided to "hire some type of computer consultant to review and see whether this was a hack or I don't know. I mean, we were very in shock that this was something that [Defendant] would do." (*Id.* at 142:1-3).

11. The Rodins met with Defendant in late August 2017 to ask her about the odd Outlook calendar deletions related to her data entries. (*Id.* at 36:13-24; 37:3-41:9; 141:21-25). Defendant specifically denied knowing about the calendar deletions. (*Id.* at 37:14-22; 144:20-25).

12. Following this late-August meeting at which Defendant denied knowing what happened to the Outlook Calendar, the Rodins placed Defendant on paid leave while they investigated the matter. (*Id.* at 144:21-145:1).

13. Victor Rodin made further discoveries during the investigation. He testified that after IFC "put her on leave, and she left, then we kind of took stock and we realized that her office was bare bones. I mean, her desk was already empty, her office which normally contained lots of files were mostly missing. I mean, three to five boxes easy worth of material was missing." (*Id.* at 142:7-11). He further discovered Defendant's personnel file was empty, (*Id.* at 131:3-23), and that her issued work laptop "had been parsed" with various emails and files missing. (*Id.* at 145:1-8). Victor Rodin stated that Defendant "is a very organized person who keeps files on everything" and therefore the discovery of all

the missing files "[was] when [the Rodins] immediately were like, we need to get this computer—something definitely is wrong here, so that's when we got the computer to the forensic IT consultant." (*Id.* at 145:6-11).

D. Forensic Investigation of Defendant's Dell Work Laptop

14. Victor Rodin testified that the forensic IT consultant revealed "evidence that she had plugged in several USB devices, I think it was six" into her work laptop, and downloaded "obviously confidential information, stuff that there was no reason for her to have." (*Id.* at 145:21-24; 146:9-15). The forensic investigation further revealed "a series of files which one of them was the spreadsheet that [] showed that she was running a side business[.]" (*Id.* at 146:18-21; *see also* Pl.'s Exs. 10, 11, 51).

15. Plaintiff's forensic IT consultant, Mr. Ashraf Massoud, testified as a qualified expert in computer forensics and examination. (*Id.* at 188:2-6, *see also id.* at 181:22-247:19; Pl.'s Ex. 49 (Expert Resume)). Mr. Massoud forensically imaged Defendant's work laptop using high speed forensic duplicators, creating a read-only copy of the hard drive. (*Id.* at 189:16-191:23). The forensic image is an exact bit-by-bit copy of the original hard drive and is "read-only," meaning that it does not alter or change the original hard drive, and preserves all the original data. (*Id.*). Mr. Massoud found that "at or around the time of when [Defendant] left employment, I saw a lot of — I saw about 20 different USB devices for example being plugged into the . . . work laptop, . . . and various files being accessed in the last week or so of August of 17." (*Id.* at 194:1-5).

16. However, Mr. Massoud was unable to determine exactly which IFC files Defendant had copied onto the USB devices. (*Id.* at 194:11-24). Mr. Massoud noted that the IFC work laptop was manufactured by Dell and employed a Windows Operating System which "will not show you how many files were copied." (*Id.* at 194:14-15). He explained that "if you just grabbed a bunch of files and dragged them from your internal C drive [(hard drive)] of your computer onto an external device, Windows does not keep any artifact that shows you that occurred. And so, in essence, where you could copy the entire hard drive . . . onto an external device and I would never know that you did that nor will I tell you how many files were done or the size or quantity of data that was taken. So Windows is real bad in that sense. There's no log that captures that information." (*Id.* at 194:16-24).

17. Mr. Massoud further explained that, to definitively figure out what information was copied from Defendant's work laptop, "the 100 percent way to do this is to actually obtain the devices that were plugged in and in a sense, we will examine those. Then I can tell you what's sitting on those devices." (*Id.* at 195:2-5). But, Mr. Massoud did not have the USB drives Defendant used to download the material because Defendant has not produced the USB drives.

18. Mr. Massoud could not definitively ascertain the full extent of the files downloaded without the USB drives themselves, but he identified certain IFC files which had been downloaded on the USB drives from Defendant's work laptop. Using a forensic software program, EnCase, Mr. Massoud examined the Dell laptop's Windows' Registry Files.

The registry files track "your settings, any user that logs into that machine, what their settings are from anything as simple as what their desktop was . . . to how many devices got plugged in, what the name of those devices are, the serial number of those devices are, the dates and times they were plugged in and it will tell me when software was installed or what kind of software was installed et cetera. So this registry is really a vast treasure [trove] so to speak of forensic information that we go through and examine." (*Id.* at 196:15-23).

19. Using EnCase and viewing the Registry Files, Mr. Massoud produced a "report called [a] USB history file access report that summarizes and shows me all the different devices that got plugged in and when and then what files were being accessed and when and then I can start correlating, okay, this file got opened when this USB drive got plugged in and we start connecting dots as to what . . . the defendant could be looking at, could be saving to various devices as a result of connecting those kind of dots." (*Id.* at 197:14-23; *see also* Pl.'s Ex. 51 (USB History File Access Report)).

20. Mr. Massoud found at least six USB drives were plugged into Defendant's work laptop during June 2017 through August 2017, immediately prior to Defendant's termination. (Pl.'s Ex. 51). The following devices were plugged into Defendant's work laptop and under her username "Odara":

    a. A Lexar USB device with serial number "AA1OR5AGNP3MCLPP" was last connected at 4:25 p.m. on August 28, 2017, the day prior to the Rodins placing Defendant on paid leave;

    b. A Lexar USB device with serial number "AAW9NN2ZB1Q1HL0S" was last connected on August 21, 2017, at 9:06 a.m.;

    c. A Lexar USB device with serial number "AA3N0789WHJDUJG" was last connected on August 17, 2017, at 11:49 a.m.;

    d. A Generic Flash Disk USB device with serial number "6ABC9652" was last connected on August 4, 2017, at 3:47 p.m.;

    e. A Lexar USB device with serial number "AA0WIM2Y0WM9ZCEA" was last connected on July 30, 2017, at 6:17 p.m.;

    f. A Lexar USB device with serial number "AABBZY5QZHHDY2W7" was last connected on June 5, 2017, at 11:56 a.m. (*Id.*).

21. Mr. Massoud identified which files Defendant accessed from her work laptop at the times that these USB drives were plugged into her laptop. (*Id.*; Tr., at 202:1-215:15). Mr. Massoud generated a list of Defendant's "LNK files" and her "Jump Lists." (Pl.'s Ex. 51; *see also* Tr., at 202:12-213:23).

22. LNK files and Jump Lists are shortcuts created by the Windows Operating System which are memorialized in the Windows Registry and track when a document or file is last accessed. (*Id.* at 203:2-205:22). For example, Mr. Massoud's USB History File Access Report shows that a "Jump List" file was created on August 28, 2017, at 2:15 p.m., entitled "RODINSERVER\Shared\Current\Documents\Property Management\Rodin Square\Rodin Square Rent Roll and Escrows.xlsx" which means that Defendant last accessed that spreadsheet from her work computer on that date while a USB drive was plugged into her work laptop. (Pl.'s Ex. 51).

23. The LNK files and Jump Lists confirmed that Defendant had downloaded IFC's information onto the USB drives. Mr. Massoud's report reveals that Defendant accessed documents which were contained on the USB drives. (Pl.'s Ex. 51).

24. For example, on July 31, 2017, at 1:54 p.m., the following files were last accessed by Defendant on USB drives: "E:\._IFC Priorities (2).doc" and "E:\._IFC Priorities FULL.doc." (*Id.*).

25. By further example, Massoud's report shows that Defendant accessed the following documents on USB drives on August 17, 2017:

    a. At 11:08 a.m., "E:\2013 checks\3 RFP LP\2013 checks – 3 RFP LP.pdf";

    b. At 11:08 a.m., "E:\2013 checks\3 RFP LP";

    c. At 11:09 a.m., "E:\2013 checks\632 N. Second LP\2013 April – June checks – 632.pdf";

    d. At 11:09 a.m., "E:\2013 checks\632 N. Second LP";

    e. At 11:10 a.m., "E:\2013 checks\2 RFP LP\2013 checks – 2 RFP LP.pdf";

    f. At 11:10 a.m., "E:\2013 checks\2 RFP LP";

    g. At 11:11 a.m., "E:\2015 checks\2 RFP LP\2015 checks – 2 RFP LP.pdf";

    h. At 11:11 a.m., "E:\2015 checks\2 RFP LP"; and

    i. At 11:11 a.m., "E:\Table of Contents for flash drive 2 orange.xlsx." (*Id.*).

26. Mr. Massoud's report showed that Defendant last accessed files using the USB drives on August 28, 2017, at 4:22 P.M., and 4:25 P.M. Defendant last accessed the files "E:\Immediate Open Items.doc" and "E:\O Topline Priorities.doc." (*Id.*). Mr. Massoud explained that "E:\" means these files were saved on, and were presently being accessed from, the external USB drives. (Tr., at 213:2-214:2).

27. Victor Rodin explained that many of the files Defendant accessed while USB drives were plugged into her laptop, as determined by Mr. Massoud's Access Report, contained IFC's confidential business information. (Tr., at 137:2-154:21; *see also* Pl.'s Exs. 37-42). For example, while Defendant had a USB drive plugged into her work laptop, she accessed "R Investment Two, LP 2017 P&L (832-834 South St.)" (Pl.'s Ex. 37), which Victor Rodin explained is a confidential profit and losses spreadsheet for IFC containing sensitive information such as: "[w]hat you're renting the tenants for each apartment, what your expenses are, how much you're making, I mean people — if someone had a property that was right nearby and wanted to undercut what rent we were, understand how we operated our property, this is like our inside information. It's as confidential as it gets[.]" (Tr., at 147:12-19).

28. Further, Mr. Massoud viewed "Shellbags" which are additional "artifacts" stored in the Window's Registry Files. (*Id.* at 215:19-23). Shellbags track when "a folder was being accessed and where that folder was and what time and day it was accessed." (*Id.* at 215:22-23).

29. Viewing the Shellbags on Defendant's work laptop, Mr. Massoud discovered "this file called FS Events" or, "File System Events." (*Id.* at 216:1-8, 11). Importantly, Defendant's work laptop was a Dell computer, and the file "FS Events" is solely created by Macintosh computers. (*Id.*). Mr. Massoud explained "[t]hat file is unusual to me because I am dealing with this Windows machine and this is an artifact of a Macintosh system, so as soon as I saw that, I knew right away that this [USB device], had also been plugged into a Macintosh machine because otherwise that file would not exist." (*Id.*). Mr. Massoud stated, "one of my first questions is if [Defendant] has a Mac and I need to examine that Mac." (*Id.* at 218:7-8). Defendant has a Macintosh computer. (*Id.* at 216:18-21; 218:5-10). Thus, Mr. Massoud concluded—because he did not have the USB drives used for downloaded the information—that "the next likely search or depository of potential data would be in her Macintosh machine that she has at home especially given the fact that we now have seen that a USB drive that was plugged into a Mac." (*Id.* at 219:1-4).

30. Based on the forensic examination of Defendant's work computer, the Rodins met with Defendant again on September 15, 2017. (*Id.* at 41:17-53:20; 154:16-157:24). The Rodins presented a severance agreement to Defendant by which the Rodins agreed to pay her some amount of her salary, and in return, Defendant would agree to: (1) return both IFC's electronic files and physical files, and (2) "stop operating her side business while using [Neal Rodin's] broker license and the IFC company brokerage license." (*Id.* at 155:12-19; *see also* Pl.'s Ex. 32).

31. At this meeting with the Rodins, Defendant denied she downloaded or took any of IFC's information and refused to sign the severance agreement. (*Id.* at 37:3-38:10; 39:19-40:13; 42:5-46:14). IFC terminated Defendant's employment. (*Id.* at 29:20-30:8; 31:7-32:9).

32. Defendant testified at the hearing that although she had downloaded IFC's information before that September 15, 2017 meeting, she did not know she had to return IFC's information. (*Id.* at 30:1-4) ("Q: Are you saying that when you were terminated from IFC, you didn't know that you had to return their confidential business records? A: Correct.").

E. Duty to Preserve Relevant Evidence: Defendant's September 19, 2017 Litigation Hold Letter and Subsequent Administrative Agency Charges

33. On September 19, 2017, Defendant's counsel sent a demand letter to IFC by way of response "to your offered Separation/Severance Agreement provided to Mrs. Jabali-Jeter, as well as outline her legal claims." (Pl.'s Mot. Contempt, ECF No. 18, Ex. C; *see also* Pl.'s Ex. 1). Defendant's counsel addressed the September 15, 2017 meeting between the Rodins and Defendant, where "[the Rodins] explained that her employment was being terminated because of 'forensic IT information,' along with running her own property management company, and presented [Defendant] with a separation/severance agreement, with a noted termination date of September 14, 2017, requesting that she return [IFC's information] by September 18, 2017." (*Id.* at 2). Defendant's counsel averred that IFC's "vague accusation regarding their purported 'IT investigation' and having her own business, smack of pretext[.]" (*Id.* at 3). Defendant's counsel maintained that "the totality of the circumstances makes clear that Mrs. Jabali-Jeter's employment was unlawfully terminated because of her pregnancy." (*Id.*).

34. Because Defendant asserted IFC terminated her because of unlawful pregnancy discrimination, Defendant's counsel also requested IFC to "please issue litigation hold letters immediately to all individuals who may have information (including electronically-stored information) relevant to these issues. As you know, the courts take preservation issues very seriously and do not tolerate spoliation." (*Id.* at 3-4). Defendant testified that she read her counsel's demand letter before it was sent, and understood and agreed with its contents. (Tr., at 74:14-75:23).

35. On September 28, 2017, Defendant filed an administrative complaint with the Pennsylvania Human Relations Commission related to "the pregnancy discrimination that ensued while [she] was employed at IFC." (*Id.* at 78:6-79:16; *see also* Pl.'s Ex. 2). In her complaint, she asserted that the Rodins terminated her on September 15, 2017, "because of forensic IT information and had accused me of improperly running my own property management company while employed by [IFC]." (Tr., at 78:15-23).

36. At the hearing, Defendant admitted that as of that date, September 28, 2017, she "still [had] in [her] possession IFC's documents and data." (*Id.* at 79:21-24). She further admitted that she "understood that [she] had to maintain and preserve all evidence related to those issues [in the administrative complaint]." (*Id.* at 80:4-6). She additionally recognized that she had a duty to maintain and preserve all evidence related to "[b]oth [her] claims and IFC's defenses." (*Id.* at 80:7-11).

37. Also in September 2017, Defendant applied for unemployment benefits. (*Id.* at 80:12-84:3). IFC filed a narrative statement opposing Defendant's application for benefits,

asserting that she had engaged in willful misconduct by deleting IFC's information, downloading and taking IFC's electronic information, and taking IFC's physical files. (*Id.* at 80:23-24, 81:13-20, 82:6-13). Defendant's application for unemployment benefits was denied because of the willful misconduct. (*Id.* at 80:25).

38. In December 2017, Defendant dual-filed charges with the Equal Employment Opportunity Commission and the Philadelphia Commission on Human Relations. (*Id.* at 84:4-86:23; *see also* Pl.'s Ex. 4). On April 19, 2018, IFC responded and stated Defendant was "terminated because [she] didn't tell them about this separate company [she was] operating and the fact that [she] had stolen documents and data from [IFC.]" (*Id.* at 86:15-23; *see also* Pl.'s Ex. 5).

39. Also, on April 19, 2018, IFC sent Defendant a cease and desist letter. (*Id.* at 87:5-89:1; *see also* Pl.'s Ex. 6). By this time, IFC had received the results of its forensic examination of Defendant's work laptop, and discovered she "systematically and without authorization or authority, connected multiple storage devices to her work laptop, copied large amounts of [IFC's] files from the work laptop to these storage devices, and then connected these storage devices to another computer not owned or operated by [IFC or the Rodins.]" (Pl.'s Ex. 6). IFC requested Defendant return all its information, tender her personal computers and storage devices for forensic examination, and cease and desist using its information in her personal real estate management business. (*Id.*).

40. Defendant's counsel responded on May 4, 2018, advising that Defendant would not tender her personal computer or storage devices for forensic examination. (Pl.'s Ex. 7; *see also* Pl.'s Mot. Sanctions, ECF No. 18-5).

F. The May 29, 2018 Temporary Restraining Order

41. On May 29, 2018, following a show cause hearing on Plaintiff's Temporary Restraining Order, the parties agreed to a consent Temporary Restraining Order. (Order, ECF No. 10; Tr., at 95:8-19, 96:20-23, 97:7-10). Most relevant to the instant matter, the TRO provided "Defendant . . . shall by no later than 10:00 a.m. on June 6, 2018" deliver all IFC's documents, materials, and other information to IFC. (Order, ECF No. 10). Further, Defendant was ordered to "preserve and take steps to prevent the automatic or intentional deletion or modification of, . . computer hard drives that may contain information related to this action[.]" (*Id.*).

G. The June 6, 2018 Production

42. On June 6, 2018, Defendant produced to Plaintiff a single flash drive containing eleven files. (*Id.* at 97:11-24, 99:22-24, 102:9-16; *see also* Pl.'s Exs. 20-28). This flash drive was not one of the six flash drives she originally used to download IFC's information, but was provided to her by her counsel. (Tr., at 99:15-18). Defendant produced the following files:

    a. AMENDMENT TO LEASE AGREEMENT.pdf;

    b. Bed Bug Addendum.pdf;

c. COMMERCIAL LEASE TEMPLATE.pdf;

d. DROPBOX CREDENTIALS.pdf;

e. Immediate Open Items.pdf;

f. Lead Paint Addendum.pdf;

g. MATERNITY LEAVE AGREEMENT copy.pdf;

h. MATERNITY LEAVE AGREEMENT.pdf;

i. MOST PERTINENT TIME SENSITIVE ITEMS.pdf;

j. O Topline Priorities.pdf; and

k. RESI Lease Template.pdf. (Pl.'s Exs. 20-28).

H. Forensic Investigation of Defendant's Personal Macintosh Laptop

43. Defendant also produced her personal Macintosh laptop for forensic imaging. Mr. Massoud's forensic investigation of Defendant's Macintosh laptop revealed evidence that Defendant downloaded information from IFC's "Rodin Server." For example, Mr. Massoud located on Defendant's laptop "2015 Federal Tax Return, Neil and Sharon Rod[i]n PDF, 2015 K1s Neil and Sharon Rod[i]n PDF, 2016 Extension Neil and Sharon Rod[i]n PDF and then 2016 Federal Tax Return [Victor Rodin].LP.PDF." (Tr., at 238:10-13; *see also* Pl.'s Exs. 46-49, 54, 99). These files were created on Defendant's laptop on "November 1st of 2017," after she was terminated on September 15, 2017. (*Id.* at 239:12-21).

44. Defendant testified that she did not know why the Rodins' tax returns were found on her laptop. (*Id.* at 118:12-14). She explained "[i]t's plausible that that information was from the information I had on my thumb drives. I don't know, but it's information that I turned over and I have no use for, no need for it, and that's why the information was given over." (*Id.* at 118:16-19). Despite her suggestion to the contrary, Defendant did not produce the Rodins' tax returns in her production on June 6, 2018, as she was required to per the TRO. (*See* Pl.'s Exs. 20-28).

45. Defendant recognized she had a duty to preserve relevant evidence and could not intentionally destroy electronic data or overwrite her laptop to destroy metadata. (*Id.* at 111:1-18). But, Mr. Massoud's forensic investigation of Defendant's personal laptop revealed evidence of tampering.

46. Mr. Massoud knew the USB drives plugged into Defendant's Dell work laptop had also been plugged into a Macintosh laptop because of the presence of the "FS Events" file. (*Id.* at 216:1-21; 218:5-10; 219:1-4). Similar to the Window's Registry Files tracking all

activity on a Windows Operating System, Mr. Massoud explained that the FS Events file, or "File System Events" is "a running log of what that [Macintosh] machine is doing and what you as a user is [sic] doing. Anything from checking your e-mail to dragging something into the trash to creating a document, whatever it is, File System Events is what tracks." (*Id.* at 220:20-23). He further provided "anything from boot up to a device that you may have connected. [FS Events] will show up as a volume and then it will give it a name to documents you've opened, documents you've renamed, documents you've dragged and dropped into the trash. The fact that you entered your trash, what program is running and then literally, almost anything that you do on that machine is tracked in that file." (*Id.* at 222:21-223:2).

47. Mr. Massoud testified that the File System Events folder on Defendant's personal laptop "was empty of data, which in my experience is extremely unusual" and "wasn't what [he] expected." (*Id.* at 220:13-19). He explained that given the extensive amount of data the File System Events file tracks, and that it is a critical and automatic tracking system in the Macintosh Operating System, "that file is empty which is, needless to say, atypical if not almost unheard of if you're using the Mac." (*Id.* at 220:24-25). He stated "[t]here [was] no user data. Nothing I was expecting . . . [i]t literally had four lines in there and that was it, the rest was empty . . . I'm going to go on a limb and say that this was probably the first case I've seen where that has happened in my experience, . . . very atypical." (*Id.* at 223:10-19).

48. Mr. Massoud ran forensic tests to ascertain why there was no data in Defendant's FS Events folder. He explained that the lack of data in Defendant's FS Events folder could be explained by a few possibilities: an individual "would have to manually turn it off," an individual "can delete that file . . . [causing it] to be emptied," an individual could "do what's called a hard crash," or an individual could "do a system update . . . any kind of a systems upgrade, will wipe that file out and then it will regenerate itself and give you a new blank one." (*Id.* at 224:13, 20-25; 225:2-6).

49. Defendant tampered with her laptop and caused the deletion of relevant tracking data on her laptop. On May 20, 2018, she initiated a major operating systems update to her personal laptop causing the deletion of data. Additionally, she took further steps resulting in the deletion of relevant data on her laptop

I. May 20, 2018: Major Operating Systems Update

50. On May 20, 2018, Defendant did several things with her personal laptop. First, she utilized the MacIntosh program "Time Machine [which] allows you to connect an external device" and copy files or even a whole hard-drive, creating a back-up. (Tr., 235:20-237:8). Defendant plugged in her external hard drive, a device entitled "Nefertiti."[1] (*Id.* at 226:4-11). After creating a copy of her laptop's hard drive, she

[1] As explained more fully below, Defendant offered to produce her back up external hard drive for forensic examination. (Tr., at 119:1-13). Mr. Massoud found that Defendant last used the back up external hard drive to make a copy of her laptop in early June 2018. (*Id.* at 237:2-4; *see also* Pl.'s Proposed Findings of Fact & Conclusions of Law, ECF No. 32, at ¶¶ 317-18).

initiated a major operating system update to her personal Macintosh laptop. (*Id.* at 226:1-18; *see also* Pl.'s Ex. 53 (Install Log)). She updated her operating system from "MacOS Sierra (10.12.6)" to "MacOS High Sierra (10.13.4)." (*Id.*; Tr., at 225:7-226:18; *see also* Pl.'s Mot. Sanctions, ECF No. 18-9, Ex. I, ¶¶10-12).

51. Mr. Massoud testified that the Macintosh laptop will prompt an individual multiple times to initiate an operating system upgrade of this kind. Defendant "had to affirmatively type in her password twice to install" the new operating system. (*Id.* at 229:14-18).

52. Mr. Massoud performed a forensic test in his lab: he upgraded a Macintosh laptop from MacOS Sierra 10.12.6 to MacOS High Sierra 10.13.4 to mirror the update Defendant initiated on May 20, 2018. (*Id.* at 227:14-228:5). The operating system upgrade "wiped out the FS Events file, so it is a major upgrade and it does a major disturbance of data on a hard drive." (*Id.* at 228:3-5).

J. Subsequent Tampering

53. Although Defendant wiped out the FS Events file on her personal laptop when she upgraded her operating system on May 20, 2018, Mr. Massoud testified regarding evidence of further tampering. (*Id.* at 230:24-231:13). Specifically, the May 20, 2018 upgrade wiped out the data in the FS Event file, "[b]ut the computer was used through June" and the FS Events file was still empty. (*Id.* at 244:22-23).

54. Defendant testified "[t]he flash drive that was turned over on June 6th was a flash drive that was provided and brought to me from counsel and they put the documents that I had in my laptop on that flash drive." (*Id.* at 99:4-7). Thus, the FS Events folder would have necessarily showed that activity. However, Mr. Massoud testified that he "didn't seen any kind of user activity such as opening documents or deleting documents or anything at all." (*Id.* at 223:12-14).

55. Mr. Massoud explained, "the fact that there is nothing in the FS Events log even though the machine was in use for a month after the [May 20, 2018] upgrade would suggest that some form of tampering had occurred. You cannot turn that machine on without FS Events being logged in. And so, I am inclined to think that the only other option there was to do — is that [FS Events] was likely deleted on a manual level to get rid of the file." (*Id.* at 245:13-19). The Court credits Mr. Massoud's unrebutted conclusion, and finds that Defendant manually deleted the FS Events file and obfuscated the tracking data.

Thus, as Mr. Massoud explained, Defendant's back up external hard drive "is a duplicate copy of the Defendant's laptop hard drive and thus likely contains the Plaintiff's confidential information, and may contain copies of the now-deleted user activity information that should have been contained within the Defendant's laptop '.fseventsd' log file/folder." (*Id.* at ¶ 319; Tr., at 237:6-21).

III. LEGAL STANDARDS

A. Motion for Sanctions

When a party from whom discovery is sought fails to comply with a court order compelling discovery, Rule 37 of the Federal Rules of Civil Procedure allow for the imposition of sanctions. The Rule provides:

> If a party . . . fails to obey an order to provide or permit discovery . . . the court where the action is pending may issue further just orders. They may include the following:
>
> (i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;
>
> (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;
>
> (iii) striking pleadings in whole or in part;
>
> (iv) staying further proceedings until the order is obeyed;
>
> (v) dismissing the action or proceeding in whole or in part;
>
> (vi) rendering a default judgment against the disobedient party; or
>
> (vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

Fed. R. Civ. P. 37(b)(2)(A).

Federal Rule of Civil Procedure 37(e), as revised by the December 1, 2015 amendments, "specifically addresses the applicability of sanctions for spoliation of [ESI]." *Accurso v. Infra-Red Servs., Inc*., 2016 WL 930686, at *3 (E.D. Pa. Mar. 11, 2016). Pursuant to Rule 37(e),

> If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
> (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e).

B. Motion for Contempt

A party seeking a civil contempt order must establish that "'(1) a valid order existed, (2) the [person at issue] had knowledge of the order, and (3) the [person at issue] disobeyed the order.'" *United States ex rel. Salvino Steel & Iron Works, Inc. v. Safeco Ins. Co. of Am.*, 181 Fed. Appx. 247, 250 (3d Cir. 2006) (*quoting John T. ex rel. Paul T. v. Del. County Intermediate Unit*, 318 F.3d 545, 552 (3d Cir. 2003)). "These 'elements must be proven by clear and convincing evidence, and ambiguities must be resolved in favor of the party charged with contempt.'" *Id.* "Thus, a contempt citation should not be granted if there is a ground to doubt the wrongfulness of the party's conduct." *In re Asbestos Products Liab. Litig.*, No. MDL 875, 2010 WL 2034636, at *4 (E.D. Pa. May 14, 2010) (*quoting Harris v. City of Philadelphia*, 47 F.3d 1342, 1346 (3d Cir. 1995)) (internal quotations omitted). A court may hold a party or non-party in civil contempt for failing to obey a subpoena or court order. *See id.*

IV. ANALYSIS AND CONCLUSIONS OF LAW

Plaintiff seeks sanctions against Defendant pursuant to Federal Rule of Civil Procedure 37(e) on the grounds that she has willfully spoliated evidence. (Pl.'s Mot. Sanctions & Contempt, ECF No. 18, at 1). Further, Plaintiff requests the Court to find Defendant in contempt of the Court's May 29, 2018 TRO. (*Id.*). The Court will first address the spoliation of evidence and appropriate sanctions. The Court next will certify facts pursuant to the Civil Contempt procedure set forth in the Federal Magistrates Act, 28 U.S.C. § 636(e)(6)(B).

A. Spoliation of Evidence

Spoliation of evidence refers to "instances where evidence has been altered or destroyed." *Bull v. United Parcel Serv., Inc.*, 665 F.3d 68, 73 (3d Cir. 2012). The spoliation analysis requires a two-part inquiry. First, the Court must determine whether spoliation occurred. Spoliation occurs where: (1) the evidence was in the party's control; (2) the evidence is relevant to the claims or defenses in the case; (3) there has been actual suppression or withholding of evidence; and (4) the duty to preserve the evidence was reasonably foreseeable to the party. *Id.*

Second, if a party did in fact spoliate evidence, the Court must determine the appropriate sanction. The Third Circuit has provided three factors to consider in determining the appropriate sanction: "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future." *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994). The burden is on the moving party "to show that spoliation occurred and what sanctions are appropriate." *Fuhs v. McLachlan Drilling Co.*, No.

16-376, 2018 WL 5312760, at *13 (W.D. Pa. Oct. 26, 2018) (quoting *Goldrich v. City of Jersey City, et al.*, 2018 WL 4492931, at *7 (D.N.J. Jul. 25, 2018)).

Plaintiff identifies three categories of evidence that were spoliated: (1) electronic copies of IFC's Information, the flash drives on which the Information was contained, and that flash drive's metadata ("Electronic Information"); (2) the physical copies of IFC's Information missing from IFC's offices ("Physical Files"); and (3) the metadata from Defendant's personal MacBook Pro laptop ("Metadata,") (collectively the "Spoliated Evidence."). (Pl.'s Prop. Findings of Fact & Concl. Of Law, ECF No. 32, at ¶ 181).

1. Spoliation Occurred

The evidence shows that Defendant spoliated three forms of evidence. She has withheld Electronic Information and the Physical Files she took from IFC's offices. Further, she willfully altered the Metadata contained on her personal laptop.

a. The Evidence was in Defendant's Control

Regarding the first element, Defendant exclusively controlled the Electronic Information, the Physical Files and the Metadata. All of these pieces of evidence were in Defendant's exclusive control. Defendant has admitted that she controlled the USB drives, and used them to download IFC's Electronic Information. (*E.g.*, Tr., at 57:19-58:8, 109:4-9, 116:8-10). Defendant now suggests that "[i]t is possible they were thrown out during the renovation [to her home]; regardless, [she] cannot locate them," but this does not rebut the contention that these USB drives were in her control. Rather, this is merely an attempt to offer reasons for her failure to produce them in this litigation. (Pl.'s Ex. 9 (Def.'s June 2018 Letter)).

We next consider the second item, IFC's Physical Files that were missing after Defendant's departure from IFC. Defendant testified that she did not take any physical files

from her office. Her testimony is rebutted by the credible testimony of Victor Rodin, who testified that Defendant's office had been "parsed," that at least 3 boxes of files were missing after Defendant's departure, and that after her departure, Defendant's own personnel file was found to be empty. (Tr., at 131:3-23; 142:7-11, 145:1-8).

As to the third item, her personal laptop and the metadata on that laptop, Defendant alone controlled that laptop.

b. The Evidence was Relevant

We next consider the second element of a spoliation claim—whether the evidence was relevant to a claim or defense—and conclude that the unproduced and altered evidence was highly relevant to Plaintiff's claims. The purloined and missing Electronic Information and Physical Files are the crux of IFC's claim: Defendant absconded with its confidential business information. Moreover, the missing USB drives are critical to understanding exactly what electronic information was taken. As Mr. Massoud explained, forensic examination of the USB drives would reveal the full scope of the electronic files downloaded from IFC's server. (Tr., at 195:2-5). Similarly, the Metadata on Defendant's personal laptop was relevant to gaining a full understanding of Defendant's usage of IFC's documents and information.

c. Defendant Suppressed and Withheld the Evidence

The third element of the spoliation inquiry addresses whether there has been actual suppression or withholding of evidence. "No unfavorable inference arises when the circumstances indicate that the document or article in question has been lost or accidentally destroyed, or where the failure to produce it is otherwise properly accounted for." *Bull*, 665 F.3d at 79 (quoting *Brewer v. Quaker State Oil Refining Corp.*, 72 F.3d 326, 334 (3d Cir. 1995)). "Therefore, a finding of bad faith is pivotal to a spoliation determination." *Bull*, 665 F.3d at 79;

see also Brewer, 72 F.3d at 334 (distinguishing between accidental spoliation and situations "indicat[ing] fraud and a desire to suppress the truth.").

Here, the Court concludes that there has been actual suppression and withholding of relevant evidence. Defendant has purposefully withheld the USB drives and Electronic Information. Mr. Massoud identified at least six USB drives which Defendant used to download IFC's information. (Pl.'s Ex. 51; *see also* Tr., at 202:1-215:15). Defendant admitted to possessing USB drives and has provided shifting explanations to their whereabouts. Relevant testimony from the hearing is as follows:

> Q: You downloaded materials on a flash drive, right?
>
> A: Yes.
>
> Q: Where are those flash drives today?
>
> A: I don't know.
>
> Q: How many flash drives did you have in your possession at any time that contained IFC's confidential and business proprietary information?
>
> A: I had two flash drives.

(Tr. at 57:19-58:1). Defendant's testimony that she had only two flash drives is contradicted by Mr. Massoud's credible expert testimony, based upon his thorough forensic examination, that she used at least six USB drives to download IFC's information. (Tr., at 197:12-203:13; *see also* Pl.'s Ex. 51 (USB File Access History Report)). She has withheld and failed to produce all of the USB drives.

Defendant contends she lost the USB drives during a home renovation. On June 18, 2018, Defendant sent a letter regarding "Explanation of Lack of Flash Drives." (Pl.'s Ex. 9 (Def.'s Spoliation Letter)). She averred: "[s]ubsequent to my termination, while pregnant, I

remodeled my home in preparation for the arrival of my newborn . . . I have searched my home and cannot locate them after an exhaustive search. It is possible they were thrown out during the renovation; regardless, I cannot locate them." (Pl.'s Ex. 9; *see also* Tr., at 122:16-123:23). Plaintiff's speculation is contradicted by the facts. Defendant had her child on September 12, 2017, and she was terminated on September 15, 2017, and admitted at the hearing that her explanation provided in her June 18, 2018 letter was false. (Tr., at 109:4-25). Moreover, she had at least one of the flash drives as of "November 1st of 2017;" the forensic examination conducted by Mr. Massoud showed that on that date, she accessed the Rodins' joint tax returns and downloaded these returns onto her personal laptop. (*Id.* at 239:12-21; *see also* Pl.'s Ex. 54, 99). I find her explanation that she misplaced the USB drives not credible. In sum, based on the totality of the evidence presented by Plaintiff, the Court concludes Defendant has withheld the USB drives to suppress evidence unfavorable to her; specifically, the evidence of how much of IFC's information and documents she downloaded. *Cf. Brown v. Certain Underwriters at Lloyds, London*, No. 16-2737, 2017 WL 2536419, at *3-4 (E.D. Pa. June 12, 2017) (discussing that the party used the allegedly "lost" phone "after it was somehow lost" and finding "that Mr. Brown's undetailed account of losing his phone is not credible and that, rather than innocently losing his phone, Mr. Brown made a deliberate choice to withhold it from production."); *First Sr. Fin. Grp. LLC v. Watchdog*, No. 12-1247, 2014 WL 1327584 at *8-9 (E.D. Pa. Apr. 3, 2014) (discussing defendant's explanations for lack of evidence and concluding "[w]hen looked at in its totality, [defendant's] course of conduct rises above mere negligence and inadvertence to effectuating actual suppression of evidence.").

Similarly, Defendant has withheld IFC's Physical Files. Victor Rodin credibly testified that after IFC "put her on leave, and she left, then we kind of took stock and we realized that her

office was bare bones. I mean, her desk was already empty, her office which normally contained lots of files were mostly missing. I mean, three to five boxes easy worth of material was missing." (Tr., at 142:7-11). He further credibly testified that Defendant's personnel file was empty, and her real estate license was missing from the wall. (*Id.* at 131:9-13, 142:22-143:6). IFC's office space was always locked; an access card was required to enter the building and a key, issued to employees only, was required to open IFC's office. (*Id.* at 144:2-16). The circumstances and evidence show that Defendant took IFC's Physical Files and has withheld those files "to suppress the truth;" i.e., to prevent IFC from determining which physical files were taken. *Brewer*, 72 F.3d at 334.

Regarding the Metadata, Defendant withheld and suppressed the metadata on her personal laptop. She tampered with the metadata on her personal laptop on May 20, 2018 when she initiated a major operating systems upgrade, thus deleting the critical tracking data in the File System Events folder. (Tr., at 224:3-232:13; *see also* Pl.'s Ex. 53). Notwithstanding the May 20, 2018 tampering, Mr. Massoud found that Defendant engaged in further tampering to obscure the critical tracking data in her File System Events Folder. As explained above, the File System Events Folder tracks all activity on the computer, and Defendant's "computer was used through June." (Tr., at 244:22-23). Yet, there was still merely "[j]ust three of four lines of . . . very vague system information . . . It literally had four lines in there and that was it, the rest was empty." (*Id.* at 223:8-9, 14-15). Significantly, Defendant testified regarding her June 6, 2018 production of a single flash drive, explaining "[t]he flash drive that was turned over on June 6th was a flash drive that was provided and brought to me from counsel and they put the documents that I had in my laptop on that flash drive." (*Id.* at 99:4-7). But, Mr. Massoud credibly testified that he "didn't seen any kind of user activity such as opening documents or deleting documents

or anything at all." (*Id.* at 223:12-14). As the FS Events Folder would have tracked and listed the documents being placed on the USB drive, this necessarily shows that Defendant engaged in further efforts to suppress the tracking metadata on her personal laptop. The Court thus credits Mr. Massoud's conclusion that Defendant "deleted on a manual level to get rid of the [File System Events] file." (*Id.* at 245:18-19).

d. The Duty to Preserve was Reasonably Foreseeable

Turning to the final element of the spoliation inquiry, the duty to preserve the evidence was reasonably foreseeable to Defendant. Defendant contests this element. In her proposed Conclusions of Law, Defendant contends her "duty to preserve relevant evidence triggered in May of 2018, not in 2017." (Def.'s Proposed Findings of Fact & Conclusions of Law, ECF No. 28, at 3). The main thrust of Defendant's argument is because she was not sued until May 21, 2018, her duty to preserve evidence did not trigger until the filing of IFC's complaint. (*Id.*). She asserts that until that date, she "was not aware that the flash drives would be relevant." (*Id.* at ¶ 18). "Defendant concedes that she possessed some number of flash drives and that they are relevant to the current action in May of 2018. However, she disputes the assertion that she spoliated evidence in bad faith." (*Id.* at ¶ 22).

Defendant's argument regarding when her duty to preserve evidence triggered is not persuasive. Her duty to preserve the relevant evidence was reasonably foreseeable to her as early as September of 2017. Arguably, her duty to preserve the Electronic Information and the Physical Files triggered the day she downloaded IFC's information on the USB drives and took the physical files from IFC's office. Defendant was certainly aware of her duty to preserve the Electronic Information and Physical Files when, on September 15, 2017, the Rodins terminated her employment because they had discovered she downloaded IFC's information and was

operating a side business. (*See* Tr., at 146:9-21; 155:12-157:6). Indeed, at the evidentiary hearing, Defendant was asked if she was "aware that these flash drives and data and documentation were relevant as far back as the day you were terminated, right?" (Tr., at 108:19-20). She responded, "I knew the information was relevant." (*Id.* at 108:21).

Moreover, her duty to preserve all relevant evidence was further cemented on September 19, 2017. On that date, Defendant's counsel sent a demand letter to IFC outlining her allegations of pregnancy discrimination, specifically noting IFC's "accusation regarding their purported 'IT investigation' and having her own business, smacks of pretext." (Pl.'s Ex. 1, at 3). Defendant's counsel requested that IFC "please issue litigation hold letters immediately to all individuals who may have information (including electronically-stored information) relevant to these issues. As you know, the courts take preservation issues very seriously and do not tolerate spoliation." (*Id.* at 4). Defendant testified that she read, understood, and agreed with the September 19, 2017 letter. (Tr., at 74:14-77:3). Accordingly, as of that date, Defendant unquestionably knew that IFC was suspicious of her conduct, and knew that "the courts take preservation issues very seriously and do not tolerate spoliation." I thus conclude that Defendant's duty to preserve the evidence was reasonably foreseeable to her.

Based on the evidence presented by IFC, as well as the testimony at the hearing, the Court finds ample evidence to support the conclusion that Defendant engaged in spoliation of evidence by (1) withholding the Electronic Information, (2) withholding Physical Files taken from IFC's office, and (3) deleting the critical tracking Metadata of the File System Events folder on her personal laptop by initiating the major operating systems update and further manually deleting the tracking metadata.

2. Spoliation Sanctions

Having found that Defendant engaged in spoliation by withholding the Electronic Information and Physical Files, and willfully tampering with the Metadata, the Court must now decide the appropriate sanction. *Bull*, 665 F.3d at 74 n.5. The Court considers three factors to determine the appropriate sanction: "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future." *Schmid*, 13 F.3d at 79.

Potential sanctions include: "dismissal of a claim or the entry of judgment in favor of a prejudiced party; the suppression of evidence; an adverse evidentiary inference, such as the 'spoliation inference'; fines; and attorney fees and costs." *AMG Nat'l Trust Bank v. Ries*, 2011 WL 3099629, at *4 (E.D. Pa. Jul. 22, 2011) (citing *Paramount Pictures Corp. v. Davis*, 234 F.R.D. 102, 110-11 (E.D. Pa. 2005)).

a. Fault

"In the wake of the Third Circuit's decision in *Bull*, a party seeking to impose sanctions for spoliation bears the burden of proving that the suppression of evidence was done in bad faith." *McCann v. Kennedy University Hosp., Inc.*, 2014 WL 282693, at *8 (D.N.J. 2014); *see also Bull*, 665 F.3d at 79. When evidence is "actually suppressed" there is a strong degree of fault that favors the imposition of sanctions. *See Brewer*, 72 F.3d at 334. Here, the evidence of Defendant's bad faith and desire to suppress the truth is strong. On numerous occasions Defendant denied having downloaded IFC's information onto USB drives. Her denials are contradicted by uncontroverted forensic evidence; yet, Defendant has failed to produce the

drives. (*E.g.*, Tr., at 154:18-155:19; *see also* Pl.'s Exs. 1-3). When she learned litigation was impending, she tampered with her personal laptop by affirmatively initiating the major operating systems update to wipe out the critical tracking features of the FS Events Folder. (Pl.'s Ex. 53; *see also* Tr., at 225:7-231:13). She further manually deleted the FS Events Folder to remove the tracking data and mask the full extent of her usage of IFC's information on her personal laptop. (*Id.* at 231:9-233:24; 244:22-245:19). Given the high degree of Defendant's fault and the fact she undertook affirmative actions to purposely obscure and destroy evidence, this factor weighs heavily in favor of sanctions.

b. Prejudice

Defendant's spoliation prejudiced IFC. The withholding of the Electronic Information and IFC's Physical Files has adversely affected IFC's ability to ascertain what files Defendant downloaded from IFC's confidential server and took from its office. Without the USB drives, Defendant has hindered IFC's efforts to figure out which files she downloaded. As Mr. Massoud explained, "the 100 percent way to do this is to actually obtain the devices that were plugged in . . . we will examine those. Then I can tell you what's sitting on those devices . . . but unless I actually look at the device itself that got plugged in, I really don't know what's on that device in its entirety." (Tr., at 195:2-9). But, Defendant has failed to produce the USB drives she admitted to using to download IFC's information. (*Id.* at 109:4-9) ("Q: How many flash drives did you have that contained [IFC's] confidential proprietary business information? A: I had two flash drives. Q: And that was not either one that you turned over, right? A: No.").

Further, the deletion of the tracking data in the File System Events Folder on her personal laptop prejudiced IFC because it prevented IFC from finding and proving the extent of IFC's information Defendant took and used herself. As Mr. Massoud explained, the Metadata from

Defendant's laptop is "is lost forever because there is [now] new data sitting on top of it and I can't get under it to see what used to be there." (*Id.* at 232:11-13). Mr. Massoud testified that to identify what files and information Defendant downloaded onto her personal laptop, he would "have to now do what's called carving data and it's a manual review process . . . [t]hat's quite [an] expensive labor intensive process." (Tr., at 232:18-233:20). Mr. Massoud generated a report of all files on Defendant's laptop, to be manually reviewed in the data carving process. (*Id.* at 234:1-235:14; *see also* Pl.'s Ex. 54). Mr. Massoud found 231,147 total files and explained "[t]his is not showing you any kind of carved data or deleted data." (Tr., at 234:14-15). Thus, to find out which of IFC's information Defendant utilized, Mr. Massoud would need to manually review the 231,147 files,[2] and then "any kind of carved data or deleted data" that he located.

Because Defendant's actions clearly prejudiced IFC, the Court finds this factor weighs in favor of sanctions. *See Gentex Corp. v. Sutter*, 827 F. Supp. 2d 384, 391 (M.D. Pa. 2011) (finding prejudice where defendants deleted electronic files and erased data off thumb drives). Defendant's spoliation has hamstrung IFC's efforts to determine which information and files she took without authorization.

c. Proportionality

"'[T]here is no rule of law mandating a particular sanction upon a finding of improper destruction or loss of evidence; rather, such a decision is left to the discretion of the Court.'" *AMG*, 2011 WL 3099629, at *4 (quoting *Paramount Pictures Corp.*, 234 F.R.D. at 111). "In choosing an appropriate sanction for the spoliation of evidence, courts should 'select the least

[2] Mr. Massoud explained that he could not use a simple keyword search of the files on Defendant's laptop. He noted that "it's very easy to hide data by just renaming it, right. You can rename it, you can even change the extension and hide data that way. So you really don't know what's in [each file] until you open it to make sure that the context is not relevant to the case." (Tr., at 235:8-14).

onerous sanction corresponding to the willfulness of the destructive act and the prejudice suffered by the victim.'" *Paramount Pictures Corp.*, 234 F.R.D. at 111 (quoting *Schmid*, 13 F.3d at 79).

Here, Plaintiff requests the Court enter default judgment against Defendant, or, alternatively, impose the "spoliation inference" against Defendant. (Pl.'s Mot. Sanctions, ECF No. 18, at 1). Further, Plaintiff requests the Court award attorneys' and experts' fees and costs associated with prosecuting the instant Motion, including the forensic review. (*Id.*). Lastly, Plaintiff requests the Court award fees and costs to be incurred from the now-required additional forensic review to cure Defendant's spoliation. (*Id.*).

I conclude that Defendant's wrongful conduct warrants sanctions, but I do not agree that an entry of default judgment against Defendant is the appropriate sanction. The Third Circuit has mandated courts select "the least onerous sanction" corresponding to the fault and prejudice of the misconduct and spoliation. Though Defendant's spoliation of evidence showed a high degree of fault and prejudice, the Court concludes that it is does not rise to the level warranting the draconian sanction of an entry of default judgment. *See, e.g.*, *TelQuest Intern. Corp. v. Dedicated Business Sys., Inc.*, 2009 WL 690996 at *3 (D.N.J. 2009) (declining to enter default judgment against defendant despite "running a 'defrag' program two days prior to delivering the computer and subsequent use of Secure Clean Software [] in direct contravention of the Court's Order."). Even without the benefit of the Spoliated Evidence, Plaintiff has obtained and developed evidence linking Defendant to the alleged misappropriation of trade secrets. While the evidence may have been stronger if Plaintiff could have obtained the Spoliated Evidence, the evidence is sufficient to proceed to trial, and provides Plaintiff with a strong basis to attempt to carry its burden of proof. This is especially true in light of the alternative sanction discussed

here. *See Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 335 n.2 (E.D. Pa. 2013) ("A sanction that has the drastic result of judgment being entered against the party who has lost or destroyed evidence must be regarded as a last resort, to be imposed only if no alternative remedy by way of a lesser, but equally efficient sanction is available." (quoting *Baliotis v. McNeil*, 870 F. Supp. 1285, 1289 (M.D. Pa. 1994) (internal quotation marks omitted))).

Under the circumstances of this case, the Court finds that the appropriate sanctions for Defendant's spoliation are: (1) levying an adverse spoliation inference sanction against her, and (2) a monetary sanctions award of associated costs and fees.[3] The spoliation inference is a "'far lesser sanction,' and is intended to level the playing field between the parties." *TelQuest Intern. Corp.*, 2009 WL 690996 at *3 (citing *MOSAID Techs., Inc. v. Samsung Electronics Co., Ltd.*, 358 F. Supp. 2d 332, 335, 338 (D.N.J. 2004)). This sanction allows the trier of fact to "receive the fact of the document's nonproduction or destruction as evidence that the party that has prevented production did so out of the well-founded fear that the contents would harm [her]." *Brewer*, 72 F.3d at 334.

This Court finds that it would be proper to instruct the jury they may infer that if Plaintiff had been given the opportunity to inspect the USB drives Defendant used or the File System Events folder on Defendant's personal laptop, any evidence would have been unfavorable to Defendant. I respectfully recommend that the District Court consider specific proposals on an adverse jury instruction and spoliation inference at or around the time of trial.

Additionally, given the Court's finding that Defendant acted in bad faith, I find that some amount of monetary sanctions may be appropriate to "compensate a party for the time and effort

[3] Of course, the Federal Magistrates Act provides that a District Judge may reconsider pretrial matters referred to magistrate judges under § 636(b)(1). *See* 28 U.S.C. § 636(b)(1).

it was forced to expend in an effort to obtain discovery" to which it was otherwise entitled. *MOSAID Techs., Inc.*, 358 F. Supp. 2d at 339. However, Plaintiff has not provided the Court with evidence of the costs and fees associated with prosecuting the instant Motion. Accordingly, Plaintiff shall submit its billing records, and/or an affidavit, within 14 days of this Order setting forth their expenses and fees incurred as a result of Defendant's spoliation of evidence. Defendant shall have fourteen days to respond.

B. Contempt

Plaintiff has requested that Defendant be held in Civil Contempt for violating Judge Jones' May 29, 2018 Temporary Restraining Order. (Pl.'s Mot. Sanctions & Contempt, ECF No. 18, at 1). Plaintiff contends that Defendant failed to deliver all its information which Defendant had in her possession, in contravention of the Order. Additionally, Plaintiff contends Defendant violated the Order by tampering with her personal laptop.[4]

1. The Magistrate Judge's Role in Contempt Proceedings

"Magistrate judges are granted contempt authority by statute." *Wallace v. Kmart Corp.*, 687 F.3d 86, 90 (3d Cir. 2012) (citing 28 U.S.C. § 636(e)). The statute provides that, except

[4] Further than the willful deletion of metadata on her personal laptop, Plaintiff seemingly argues Defendant should be held in contempt for using her back-up external hard drive "to create a hard drive backup on June 6, 2018, the deadline for Defendant to comply with the Court's Order." (Pl.'s Proposed Findings of Fact & Conclusions of Law, ECF No. 32, at ¶ 318). Defendant explained that "my laptop was my sole – one of the sole tools I used for, you know, my income and my livelihood and in the event, it got damaged or lost or stolen, I wanted to make sure I had a copy of it so that I can replace it." (Tr., at 119:5-10). Understandably, before tendering her personal laptop for forensic examination, Defendant wanted to preserve her data. This action was not taken in bad faith or in contravention of the Court's Temporary Restraining Order. However, as Defendant testified, she is "willing to turn [her back up hard-drive] over immediately." (*Id.* at 119:12-13). Because Defendant tampered with the tracking metadata on her personal laptop, she shall produce her external back up hard drive for forensic examination, as this hard-drive may contain IFC's information or copies of the now-deleted File System Events folder.

where a Magistrate Judge exercises consent jurisdiction in civil cases under 28 U.S.C. § 636(c) or misdemeanor jurisdiction under 18 U.S.C. § 3041, the Magistrate Judge may not enter an order of civil contempt. Instead, Section 636(e)(6)(B) sets forth the applicable authority and procedure:

> "[T]he magistrate judge shall forthwith certify the facts to a district judge and may serve or cause to be served, upon any person whose behavior is brought into question under this paragraph, an order requiring such person to appear before a district judge upon a day certain to show cause why that person should not be adjudged in contempt by reason of the facts so certified. The district judge shall thereupon hear the evidence as to the act or conduct complained of and, if it is such as to warrant punishment, punish such person in the same manner and to the same extent as for a contempt committed before a district judge."

28 U.S.C. § 636(e)(6)(B).

The Third Circuit has explained "'under the statute, the magistrate judge's certification of facts seems designed to serve function of a charging instrument or pleading for a trial to be held before the district judge.'" *Wallace*, 687 F.3d at 90 (quoting *Taberer v. Armstrong World Indus., Inc.*, 954 F.2d 888, 903 (3d Cir. 1992)). Once the facts are certified, "[t]he statute clearly specifies that the order to show cause shall require the alleged contemnor to appear before a judge of the district court, who hears the evidence . . . and decides whether to impose punishment." *Taberer*, 954 F.2d at 903.

"Proof of contempt requires a movant to demonstrate '(1) that a valid order of the court existed; (2) that the defendants had knowledge of the order; and (3) that the defendants disobeyed the order.'" *F.T.C. v. Lane Labs-USA, Inc.*, 624 F.3d 575, 582 (3d Cir. 2010) (quoting *Marshak v. Treadwell*, 595 F.3d 478, 485 (3d Cir. 2009)). These elements must be proven by "'clear and convincing' evidence." *Id.* (quoting *John T. v. Del. Cnty. Intermediate Unit*, 318 F.3d 545, 552 (3d Cir. 2003)).

2. Contempt for Violation of Court's Temporary Restraining Order

I certify the following facts relating to the issue of whether Defendant is in contempt for failure to comply with Judge Jones' May 29, 2018 Temporary Restraining Order:

1. On May 29, 2018, Judge C. Darnell Jones II issued a Temporary Restraining Order, directing Defendant to preserve evidence including, *inter alia*, all databases, electronic files, emails, media, and computer hard drives. (Order, ECF No. 10). Further, Defendant was ordered to produce all IFC's business information and records no later than June 6, 2018, at 10:00 a.m. (*Id.*). Defendant admitted she read and understood the Temporary Restraining Order. (Tr., at 95:8-96:23).

2. Mr. Massoud credibly testified that both before and after the May 29, 2018 Temporary Restraining Order, Defendant took active steps to delete critical tracking metadata located in the File System Events folder on her personal laptop. (*Id.* at 231:3-13; 237:2-24; 241:22-242:8; 245:13-19). Defendant caused the tracking data in the File System Events folder to be deleted when she initiated a major operating systems upgrade to her laptop on May 20, 2018. (Pl.'s Ex. 53; *see also* Tr., at 223:8-226:18; 227:11-231:2). This affirmative installation to delete the tracking metadata occurred before the Court's Temporary Restraining Order, but places into context the deletion of the tracking metadata occurring after the Court's Order.

3. After the May 20, 2018 major operating system upgrade, Defendant took further active steps to delete the tracking data in her personal laptop's File System Events folder, in contravention of the Court's May 29, 2018 Order. Mr. Massoud credibly testified that the evidence on Defendant's laptop revealed she used the laptop through June. (*Id.* at 244:22-23).

4. Indeed, Defendant testified "[t]he flash drive that was turned over on June 6th was a flash drive that was provided and brought to me from counsel and they put the documents that I had in my laptop on that flash drive." (*Id.* at 99:4-7). Thus, at some point in June 2018, the File System Events Folder on her personal laptop would have tracked the placing of those files from her laptop onto the flash drive she produced.[5]

5. Mr. Massoud testified that he "didn't seen any kind of user activity such as opening documents or deleting documents or anything at all" which necessarily would have been

[5] Mr. Massoud also found that, in early June 2018, Defendant used her back up external hard-drive to create a copy of her laptop's hard-drive. (Tr., at 237:2-4; Pl.'s Ex. 50, ¶¶ 16-18). I find that Defendant undertook this action merely to preserve her laptop's data before tendering it for forensic examination. However, the creation of the back-up nonetheless would have been tracked in the File System Events folder on her personal laptop. Given that Mr. Massoud found only three lines of data in the FS Events folder, and no tracking data for the copying of files onto her external back up hard drive, this is further evidence supporting the conclusion she manually deleted the folder to mask the full extent of her data usage.

tracked in the folder. (*Id.* at 223:12-14). Accordingly, Mr. Massoud concluded, "the fact that there is nothing in the FS Events log even though the machine was in use for a month after the [May 20, 2018] upgrade would suggest that some form of tampering had occurred. You cannot turn that machine on without FS Events being logged in. And so, I am inclined to think that the only other option there was to do — is that [FS Events] was likely deleted on a manual level to get rid of the file." (*Id.* at 245:13-19). I find that Mr. Massoud's credible testimony establishes that Defendant manually deleted the File System Events folder on her personal laptop after the Court's May 29, 2018 Temporary Restraining Order directed her not to delete such data.

6. Further, in examining Defendant's personal laptop, Mr. Massoud found the documents "2015 Federal Tax Return, Neil and Sharon Rod[i]n PDF, 2015 K1s Neil and Sharon Rod[i]n PDF, 2016 Extension Neil and Sharon Rod[i]n PDF and then 2016 Federal Tax Return [Victor Rodin].LP.PDF." (Tr., at 238:10-13; *see also* Pl.'s Exs. 46-49, 54, 99). These files were created on Defendant's personal laptop on November 1, 2017, and were last accessed on May 20, 2018. (Pl.'s Ex. 54 (Tabs 121489-93)).

7. Defendant testified that she did not know why the Rodins' tax returns were found on her laptop. (*Id.* at 118:12-14). She explained "[i]t's plausible that that information was from the information I had on my thumb drives. I don't know, but it's information that I turned over and I have no use for, no need for it, and that's why the information was given over." (*Id.* at 118:16-19).

8. In her June 6, 2018 production of documents pursuant to Judge Jones' Temporary Restraining Order, Defendant did not turn over the Rodins' tax returns which were located on her personal laptop. (*See* Pl.'s Exs. 20-28 (Defendant's June 6, 2018 Production)).

V. CONCLUSION

For the foregoing reasons, this Court finds Defendant engaged in spoliation of evidence by withholding USB drives and physical files, and willfully tampering and deleting metadata on her personal laptop. Accordingly, the Court finds that specific proposals for adverse "spoliation inference" are appropriately considered by the District Judge at time, or near, time of trial. The Court further finds that some amount of compensatory monetary sanctions are warranted. Plaintiff shall submit its billing records, and/or an affidavit, within 14 days of this Order setting forth their expenses and fees incurred as a result of Defendant's spoliation.

Additionally, this Court finds that Plaintiff has established a prima facie case of Civil Contempt of Judge Jones' May 29, 2018 Temporary Restraining Order, and thus certifies the facts, set forth above, to the District Court for a hearing and determination on Plaintiff's Motion for Contempt.

Accordingly, Plaintiff's Motion for Sanctions and Contempt is GRANTED. Further, pursuant to 28 U.S.C. § 636(e)(6)(B), this Court certifies the facts constituting a prima facie case of Civil Contempt and orders Defendant Odara Jabali-Jeter to appear before the Honorable C. Darnell Jones II for a hearing to show cause why she should not be held in contempt.

An appropriate Order follows.

BY THE COURT:

/s/ Lynne A. Sitarski
LYNNE A. SITARSKI
United States Magistrate Judge