IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

HCC INSURANCE HOLDINGS, INC., **Plaintiff,** **v.** **VALDA FLOWERS, CREATIVE RISK UNDERWRITERS, LLC, MICHAEL REMEIKA,** **Defendant.**	**1:15-cv-3262-WSD**

OPINION AND ORDER

This matter is before the Court on Plaintiff HCC Insurance Holdings, Inc.'s ("HCC") Motion for Spoliation Sanctions [85].

I. BACKGROUND

This case arises out of Defendants Valda Flowers' ("Flowers") and Michael Remeika's ("Remeika") resignation from non-party HCC Life Insurance Company ("HCC Life") and their operation of a competing business, Creative Risk Underwriters, LLC ("CRU") (together with Flowers and Remeika, "Defendants"). On September 16, 2015, HCC initiated this action, claiming that Flowers, at the direction of Remeika, misappropriated HCC's trade secrets to establish CRU and compete with HCC.

A. Flowers' Activity

1. Email Activity

On August 11, 2015, 8,683 emails from Flowers' HCC Life email account were moved to her H: Drive on HCC's network. (Mot. at 3).[1] 1,384 of those emails were then deleted. (Id.). HCC claims this activity was suspicious, including because Flowers had never moved emails to her H: Drive before, her email box was nowhere near full capacity, and she deleted emails from this email box on the same day. (Mot. at 3-4). HCC's former employee, Shalla Miguez, testified that she helped Flowers move the emails after Flowers asked her to help clean up her inbox, and to show her how to create folders to save relevant emails. (Miguez Dep. [92.8] at 63:17-65:2).

2. Hot Sheet Activity

On August 12, 2015, Flowers copied around 500 "Hot Sheets" from HCC Life's underwriting drive to her H: Drive on HCC's network, and then to the local C: Drive of her HCC computer. (Mot. at 5). HCC claims this activity was suspicious because it was not part of her job duties to update HCC's Hot Sheets, and because, prior to August 12, 2015, Flowers only had four Hot Sheet folders

[1] The Court's citations to the parties' briefs incorporate the depositions and other evidence on which the parties rely.

located in the C: Drive of her HCC computer. (Id.). Defendants claim that updating Hot Sheets was part of Flowers' regular job duties, and note that, on the same day the Hot Sheets were moved, Flowers received an email requesting that all Hot Sheets be updated. Defendants also note that Flowers' history of working with Hot Sheets shows she often copied them to her local HCC computer. (Resp. [92] at 6-7).

On August 20, 2015, the night before she resigned, Flowers deleted over 500 Hot Sheets from the C: Drive of her HCC computer. HCC claims this activity is suspicious because a forensic review of Flowers' past practices showed no evidence of any other mass deletions of documents. (Mot. at 5-6). Defendants note that all of the "deleted" Hot Sheets were in the recycle bin of Flowers' HCC laptop, and that HCC had the ability to retrieve the files. (Resp. at 7).

3. Return of HCC Computer

On Friday, August 21, 2015, Flowers emailed her resignation letter to her supervisor at HCC Life. That afternoon, HCC Life's Human Resources Manager, Tim Swoger, called Flowers three times to request that she return her HCC computer. (Mot. at 6). Flowers returned her computer around 4:15 p.m. that day, after asking Mr. Swoger whether she could keep her HCC computer over the weekend. (Id.). HCC claims this activity was suspicious, including because

Flowers logged into HCC Life's networks remotely after 10 p.m. the night before she resigned, and again throughout the day of her resignation. (Id. at 6-7). Defendants contend that Flowers was attempting to access the HCC network to complete her expense report, because she had $1,272.00 in reimbursable expenses and she had not submitted an expense report since June 2015. (Resp. at 7-8).

B. Mr. Flowers

Flowers' husband, Jeff Flowers, is an experienced IT professional with 35 years of experience, and he assisted CRU with IT matters. (Mot. at 7). HCC claims Mr. Flowers helped Flowers misappropriate HCC trade secrets. HCC claims Mr. Flowers "could have utilized several methods to transfer HCC's trade secrets to [Flowers'] personal devices without leaving any evidence on her HCC computer," including by using Gmail, using Citrix, or by imaging the hard drive of Flowers' HCC computer. (Mot. at 7).

C. Duty to Preserve Timeline

On August 27, 2015, Flowers received a "preservation notice" letter from HCC, requesting Flowers to retain all electronic evidence, including electronic storage devices. Mr. Flowers was aware that Flowers received the letter. (Resp. at 10-11). On September 17, 2015, Flowers received a copy of the Complaint in this action and was aware that (a) HCC was requesting Flowers turn over her personal

laptop and all electronic storage devices; and (b) that all electronic data on Flowers' personal computer was required to be retained. On September 21, 2015, the Court held a hearing on HCC's request for a temporary restraining order. The same day, the Flowers were informed that the Court ordered Ms. Flowers to produce her personal computer for examination by a neutral forensic examiner (the "Neutral"). (See Mot. at 8-9).

D. Allegedly Destroyed Evidence

HCC claims that, after receiving the lawsuit papers in this case, and after the Court ordered Flowers to produce her personal computer, Defendants destroyed: (1) data on Flowers' personal laptop; and (2) a thumb drive that was plugged into Flowers' personal computer on September 20, 2015 ("Thumb Drive").

1. Thumb Drive

Mr. Flowers claims he inserted his personal Thumb Drive on September 20, 2015, to back-up data on Flowers' personal laptop, that the Thumb Drive was corrupted and did not work, and that he therefore threw it away. Mr. Flowers tried to plug the Thumb Drive into the laptop twice, but the computer did not appear to recognize the Thumb Drive since he did not see an auto-popup or auto-play message. (Resp. at 12). Mr. Flowers believed the Thumb Drive was

defective, and he discarded the Thumb Drive the same day by throwing it into the trash. (Id. at 12). HCC contends Mr. Flowers' claim is contradicted by Defendants' own computer forensic expert, who confirmed that, the second time Mr. Flowers inserted the thumb drive, it worked properly. The second time Mr. Flowers plugged it in, he removed it after 38 seconds. (Resp. at 13). Two days later, on September 22, 2015, Mr. Flowers used a different thumb drive to copy iTunes and photograph folders that he claims he intended to copy on September 20, 2015. (Resp. at 13).

2. Personal Computer

On September 19, 2015, and again on September 22, 2015, the day after the Court ordered Flowers to produce her personal computer, the computer wiping program CCleaner was manually run on Flowers' personal laptop. (Mot. at 11). CCleaner is a program that can be used to clean the registry of a computer, which becomes corrupted during updates to the computer. (Resp. at 14). The parties disagree how often the CCleaner program was run manually, with Defendants contending it had been run manually at least fifteen (15) times, and HCC claiming the program had only been run manually once before in September 2013. HCC also claims the program was run a total of eleven times from September 19 through September 22, whereas it had previously only been run a total of four times.

(Reply [99] at 1-2). During the time period of September 19 through September 22, 2015, the laptop had a "blue screen" crash, and there was an update to Windows and/or the iTunes program. Mr. Flowers claims he ran the CCleaner registry cleaning function to get the laptop to properly run. (Resp. at 15). Defendants claim the laptop is an unstable machine that frequently crashes, and was originally purchased in 2008. (Resp. at 12). Because of its unreliability, Defendants claim they use it mostly to store Flowers' iTunes account and photograph folders. (Id.).

HCC claims that, on September 22, 2015, a program called Defraggler was run on the laptop. (Mot. at 14). Defraggler is a program that overwrites deleted files in unallocated space on a computer's hard drive. Mr. Flowers used Defraggler routinely on the laptop for maintenance, and Defendants contend that the last time Defraggler was used on the laptop was on June 9, 2015, months before the events relevant to this action. (Resp. at 15).

On September 24, 2015, the day before Flowers turned her personal computer over to the Neutral, a program called WinUndelete, which is used to recover deleted files, was run on her personal computer. (Mot. at 14-15). HCC claims Mr. Flowers used WinUndelete to confirm that he had destroyed evidence.

(Id.). Mr. Flowers claims he ran the program off of his work thumb drive to familiarize himself with it for future use for work purposes. (Resp. at 15-16).

E. Discovery and Forensic Examinations

During discovery, Flowers turned over all of her personal and work computers, electronic storage devices, email accounts and cloud storage accounts to Greg Freemyer, the Neutral jointly selected by the parties. (Resp. at 3). After running extensive searches over several weeks, the Neutral did not locate any HCC confidential information or trade secrets. (Id. at 3-4). The parties then sent all of the data collected by the Neutral to each party's respective forensic expert. HCC's forensic expert, Davis Roose, did not identify any document, information, files, or other data taken from HCC by Flowers. (Id. at 4).

HCC subpoenaed Google, Microsoft, and Citrix to produce emails and documents from Flowers', Remeika's, and Mr. Flowers' accounts from May 2015 through November 2015, and deposed several witnesses, including Mr. Flowers and his son. (Id.). HCC has not presented any evidence that HCC's Hot Sheets or other sensitive information were resident on any electronic device or storage medium in Flowers' custody, possession, or control. It claims that Flowers and Mr. Flowers, "through the sophisticated use of computer applications designed to transfer, delete and permanently destroy information, . . . effectively cover[ed]

their tracks to make it impossible to determine exactly what HCC information they misappropriated and how they used it." (Reply at 2). HCC contends this alleged misconduct warrants an adverse inference.

II. DISCUSSION

A. Legal Standard

"Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." Graff v. Baja Marine Corp., 310 F. App'x 298, 301 (11th Cir. 2009) (internal quotation marks omitted) (quoting West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999)). A party seeking spoliation sanctions must prove that (1) the missing evidence existed at one time; (2) the defendant had a duty to preserve the evidence; and (3) the evidence was crucial to the plaintiff's prima facie case. Marshall v. Dentfirst, P.C., 313 F.R.D. 691, 694 (N.D. Ga. 2016) (citing In re Delta/AirTran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1305 (N.D. Ga. 2011)). In considering the particular spoliation sanction to impose, "courts should consider the following factors: (1) prejudice to the non-spoiling party as a result of the destruction of evidence, (2) whether the prejudice can be cured, (3) practical importance of the evidence, (4) whether the spoiling party acted in good or bad faith, and (5) the potential for abuse of expert

testimony about evidence not excluded." In re Delta, 770 F. Supp. 2d at 1305 (citing Flury v. Diamler Chrysler Corp., 427 F.3d 939, 945 (11th Cir. 2005)).

Even if the Court finds spoliation, a sanction of default or an instruction to the jury to draw an adverse inference from the party's failure to preserve evidence is allowed "only when the absence of that evidence is predicated on bad faith." Bashir v. Amtrak, 119 F.3d 929, 931 (11th Cir. 1997). A showing of bad faith requires the plaintiff to demonstrate that a "party purposely loses or destroys relevant evidence." Id. Mere negligence in destroying evidence is not sufficient to justify striking an answer. See Mann v. Taser Int'l, Inc., 588 F.3d 1291, 1310 (11th Cir. 2009). In determining whether to impose sanctions for spoliation, "[t]he court should weigh the degree of the spoliator's culpability against the prejudice to the opposing party." Flury, 427 F.3d at 946.

Effective December 1, 2015, Rule 37(e) of the Federal Rules of Civil Procedure was amended to establish the findings necessary to support certain curative measures for failure to preserve electronically stored information.[2] This

[2] The version of Rule 37(e) effective at the time Plaintiff filed initiated this action stated: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

amendment "forecloses reliance on inherent authority or state law to determine when certain measures should be used" to address spoliation of electronically stored information. See Fed. R. Civ. P. 37(e), Advisory Committee Note to 2015 Amendment. Amended Rule 37(e) provides:

> **Failure to Preserve Electronically Stored Information.** 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).[3]

[3] This version of Rule 37(e) applies to civil cases commenced after December 1, 2015, "and, insofar as just and practicable, all proceedings then pending." See 2015 US Order 0017; 28 U.S.C. § 2074(a). Though Plaintiff initiated this action before December 1, 2015, the parties do not contest that the current version of Rule 37(e) applies here, and the Court concludes that applying

B. Analysis

Flowers was under a duty to preserve evidence on her laptop when she received HCC's August 27, 2015, letter directing her to "preserve any evidence that may be relevant to any of the matters referenced in this letter, including . . . hard drives of any computers to which you have access (including both personal and work computers), and any electronic storage devices which you have used or to which you have access . . ." ([92.17]). Though Flowers' and her husband's actions are troubling, and in breach of her duty to preserve, the Court finds spoliation sanctions are not warranted.

HCC's Motion is based on a series of events it casts as suspicious, but HCC offers only bare speculation that any of its trade secrets or other data were actually transferred from HCC Life's systems to Flowers' personal laptop. A party seeking spoliation sanctions must prove that (1) the missing evidence existed at one time; (2) the defendant had a duty to preserve the evidence; and (3) the evidence was crucial to the plaintiff's prima facie case. Marshall, 313 F.R.D. at 694 (citing In re

---

the amended version of Rule 37(e) would be just and practicable, including because the amended to Rule 37(e) does not create a new duty to preserve evidence. See Fed. R. Civ. P. 37(e), Advisory Committee Note to 2015 Amendment ("Rule 37(e) does not purport to create a duty to preserve. The new rule takes the duty as it is established by case law, which uniformly holds that a duty to preserve information arises when litigation is reasonably anticipated."); see also Marshall v. Dentfirst, P.C., 313 F.R.D. 691, 696 (N.D. Ga. 2016).

Delta, 770 F. Supp. 2d at 1305). Regarding the first element, "[i]t is axiomatic that in order for there to be spoliation, the evidence in question must have existed and been in the control of a party." Wilder v. Rockdale Cty., No. 1:13-CV-2715-RWS, 2015 WL 1724596, at *3 (N.D. Ga. Apr. 15, 2015) (quoting Sentry Select Ins. Co. v. Treadwell, 734 S.E.2d 818, 848 (Ga. Ct. App. 2012)).[4]

Here, after extensive discovery, including examinations by a neutral forensic examiner and the parties' expert forensic examiners, depositions, and subpoenas of email and cloud-based storage companies, HCC does not provide any evidence to show that Flowers or her husband actually transferred any data from HCC Life to her personal devices or cloud storage media she controlled. HCC argues that Mr. Flowers "could have utilized several methods to transfer HCC's trade secrets to [Flowers'] personal devices without leaving any evidence on her HCC computer," including by using Gmail, using Citrix, or by imaging the hard drive of Flowers' HCC computer. (Mot. at 7). But HCC does not present any evidence that Mr. Flowers in fact did so. HCC thus fails to show that any of its data was

[4] "The Eleventh Circuit has discussed and relied on Georgia state law in spoliation cases, even though federal law applies to the issue of spoliation sanctions, because 'Georgia state law is wholly consistent with federal spoliation principles.'" Wilder, 2015 WL 1724596, at *3 n.1 (quoting Flury v. Daimler Chrysler Corp., 427 F.3d 939, 944 (11th Cir. 2005).

resident on any of Flowers' or Mr. Flowers' personal devices or was otherwise in their control.

HCC relies on several nonbinding cases to argue that the timing of Mr. Flowers' use of CCleaner and other programs is sufficient to establish that spoliation sanctions are warranted. These cases do not apply, because it was undisputed in each case that relevant information existed on the destroyed devices. For instance, in Taylor v. Mitre Corp., No. 1:11-cv-1247, 2012 WL 5473573 (E.D. Va. Nov. 8, 2012), the plaintiff, after securing counsel to bring a discrimination lawsuit against his employer, wiped his work desktop, then took a sledgehammer to it and disposed of it in the local landfill. Id. at *1. It was undisputed that "[t]he work computer contained copies of his work-related emails," and that the plaintiff transferred some of the data from his work computer to his personal laptop. After the court ordered him to submit the laptop for inspection, plaintiff downloaded and ran a program called "Evidence Eliminator" as well as CCleaner at least twice between the order and the inspection. Id. at *1-2. Taylor does not apply here because it was undisputed that the plaintiff had transferred relevant documents from his work computer to his personal laptop before using wiping programs. Similarly, in Se. Mech. Servs., Inc. v. Brody, 657 F. Supp. 2d 1293 (M.D. Fla. 2009), the court awarded spoliation sanctions where the defendants wiped emails,

text messages, and other data from their work Blackberries. The court noted that the party seeking sanctions first must prove that "the evidence existed at one time," and found that, because the defendants used their Blackberries for work purposes, it was "clear that evidence existed at one time . . . ." Id. at 1299; see also Internmatch, Inc. v. Nxtbigthing, LLC, No. 14-CV-05438-JST, 2016 WL 491483 (N.D. Cal. Feb. 8, 2016) (defendants violated duty to preserve in trademark action where defendant testified that documents showing his prior use of the mark were resident on a company computer "which was discarded months after litigation began," allegedly because the hard drive was destroyed by a power surge).

The Court also finds HCC's reliance on Barrette Outdoor Living, Inc. v. Mich. Resin Representatives, No. 11-13335, 2013 WL 3983230, at *16 (E.D. Mich. Aug. 1, 2013) is misplaced. In Barrette, the court awarded spoliation sanctions where a defendant disposed of his cell phone and wiped his personal computer of relevant documents. The court noted that the defendant, only "a few hours after" plaintiff made "severe allegations" justifying legal counsel, went to a Sprint store to change his cell phone contract. The defendant claimed he had turned in his old cell phone as a condition for receiving a new phone, but Sprint stated that it does not require a subscriber to turn in old cell phones. The defendant also claimed he switched his contract to save money, but the evidence showed he

actually entered into a more expensive contract. With respect to the laptop, the evidence showed the defendant used CCleaner to wipe 270,000 files from his laptop one week after the court ordered him to produce his laptop for imaging. Defendant, who built his own computers and touted his computer knowledge, claimed, all evidence to the contrary, that running cleaning software would make the imaging of his laptop less expensive. Though the court found the "temporal proximity" of the defendant's actions "play[ed] a large role[,]" the court also found the defendant's explanations for his actions wholly incredible. Id. at *15.

Unlike in Barrette, the Court here finds Mr. Flowers' explanations generally consistent with the forensic evidence. Defendants show that Mr. Flowers attempted to use the Thumb Drive to save personal files and photographs, that he discarded it upon belief that it did not function, and that he did not copy anything onto the Thumb Drive. Flowers herself had no knowledge of or access to the Thumb Drive, which was owned by Mr. Flowers. (See Mr. Flowers Decl. ¶¶ 5-11; Flowers March Dep. 119:7-9, 123:10-16). Though there is some evidence to show the Thumb Drive functioned when Mr. Flowers inserted it a second time, it was only inserted for 38 seconds. He also testified that, two days later, he used a different thumb drive to copy the iTunes and photograph folders he claims he intended to copy on September 20, 2015. Regarding the use of CCleaner, that the

laptop, which was purchased in 2008, experienced a "blue screen" crash and a system or iTunes update during the relevant time period supports Mr. Flowers' claim that he ran CCleaner to restore the laptop's functionality. Unlike in Barrette, where the evidence showed a large number of files were deleted, HCC does not present any evidence to show that CCleaner was used to wipe large numbers of documents. CCleaner can be used to selectively delete internet browsing history, cookies, recycle bin documents, log files, application data, autocomplete form history, and other data. (See www.piriform.com/ccleaner/version-history). As Defendants' expert shows, CCleaner on Ms. Flowers' laptop was very near to a default configuration, meaning that, while there were many options that could have been manually enabled to destroy key forensic artifacts, these options were not enabled. This is consistent with Mr. Flowers' testimony that he used CCleaner as a registry cleaner, not to wipe data. (See [92.3] ¶¶ 23-5).[5] In sum, even if temporal proximity in combination with inconsistent or suspect explanations were enough to establish that spoliation occurred, HCC fails to present evidence to cast significant doubt on Mr. Flowers' stated reasons for his actions.

[5] The Court also credits the Defendants' expert's report that Defraggler was not run on September 22, 2015, or since June 9, 2015. (See id. ¶¶ 27-30).

HCC has not shown that the evidence it claims Flowers destroyed was resident on Flowers' personal laptop or on a cloud-storage service in her control. HCC thus fails to meet its burden to show spoliation sanctions are appropriate here.

III. CONCLUSION

For the foregoing reasons,

IT IS HEREBY ORDERED that HCC Insurance Holdings, Inc.'s Motion for Spoliation Sanctions [85] is **DENIED**.

SO ORDERED this 30th day of January, 2017.

WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE