UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 18-80994-Civ-Brannon

NITV FEDERAL SERVICES, LLC,

Plaintiff,

vs.

DEKTOR CORPORATION, and
ARTHUR HERRING III,

Defendants.

_____/

ORDER GRANTING PLAINTIFF'S MOTION FOR SANCTIONS FOR SPOLIATION OF EVIDENCE AND DISCOVERY ABUSE

THIS CAUSE is before the Court on Plaintiff's Motion for Sanctions Against Herring for Spoliation of Evidence and Discovery Abuse [DE 103]. Defendant Herring has responded in opposition [DE 119], Plaintiff has replied [DE 120], and Defendant Herring has filed an unauthorized sur-reply[1] [DE 126]. The Court has independently reviewed the entire record in this matter and is fully advised. For the following reasons, the Court finds that the extraordinary circumstances presented call for extraordinary action. Plaintiff's Motion is granted.

I. BACKGROUND

This case involves two competing businesses that sell truth verification technology. NITV is a Florida limited liability company based in Palm Beach County whose members

[1] Under S.D. Fla. L.R. 7.1(c), after a reply is filed, "[n]o further or additional memoranda of law shall be filed without prior leave of Court." Although Mr. Herring did not seek leave of Court to file his sur-reply, the Court has nonetheless considered it in analyzing Plaintiff's motion for spoliation sanctions.

are all Florida citizens [DE 1 ¶ 1]. Dektor is a Pennsylvania corporation headquartered in Coopersburg, Pennsylvania [*Id.* ¶ 2]. Dektor's President and sole shareholder is Defendant Arthur Herring III, who is a citizen and resident of Pennsylvania [*Id.* ¶¶ 3, 22].

On July 27, 2018, NITV filed this lawsuit alleging four counts against Dektor and Mr. Herring: false advertisement, unfair competition, and product disparagement under the Lanham Act, 15 U.S.C. § 1125(a) (Count I), deceptive and unfair trade practices under Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA") (Count II), defamation/business disparagement (Count III), and tortious interference (Count IV) [DE 1]. Generally, NITV alleges that Dektor unfairly competes with NITV by making false and defamatory statements about NITV, NITV's founder, and NITV's CVSA product to gain an unfair advantage in the market [DE 1 ¶¶ 29-86]. NITV alleges that the false and defamatory statements have been (1) published on Dektor's website, (2) communicated by Mr. Herring on behalf of Dektor in emails and on phone calls with several different law enforcement agency contacts across the U.S., (3) made by Mr. Herring on behalf of Dektor during a speech at a polygraph summit in Texas, and (4) made to organizers of a "Crimes Against Children" conference at which NITV was scheduled to speak [*Id.*]. NITV alleges that the false and disparaging statements have caused incredible damage to NITV's reputation, goodwill, and sales—causing damages "estimated to exceed $7 million." [*Id.* ¶¶ 35, 83, 85].

On March 12, 2019, a Clerk's default was entered against Dektor based upon its failure to appear, answer, or otherwise plead to NITV's Complaint, despite having been duly served [DE 85]. On April 1, 2019, pursuant to 11 U.S.C. § 362(a)(1), the Court stayed this case as to Mr. Herring only based upon Mr. Herring's filing of a bankruptcy petition

on behalf of himself individually in a Pennsylvania bankruptcy court [DE 92]. The Court expressly noted that this case would proceed against Dektor [*Id.*].

On May 17, 2019, the Court issued an order of final default judgment against Dektor as to liability only with instructions for Plaintiff to submit supplemental evidence regarding the appropriate amount of damages [DE 95]. The Court further granted permanent injunctive relief against Dektor [*Id.*]. Shortly thereafter, on May 31, 2019, pursuant to 11 U.S.C. § 362(a)(1), the Court stayed this case as to Dektor based upon notice that Dektor had initiated a bankruptcy case in a Pennsylvania bankruptcy court [DE 98].

On June 7, 2019, this case was re-opened and the stay against Mr. Herring was lifted based upon the bankruptcy court's dismissal of Mr. Herring's bankruptcy case [DE 107]. On June 14, 2019, the stay against Dektor was similarly lifted based upon the bankruptcy court's dismissal of Dektor's separate bankruptcy case [DE 107].

Meanwhile, on June 10, 2019, NITV filed the instant motion seeking the imposition of a default against Mr. Herring. As grounds, NITV argues:

> The Motion seeks an admittedly harsh remedy against Herring –the entry of default and/or striking of pleadings – as a result of a multitude of egregious discovery violations that . . . include: (a) Herring's installation and use of permanent file-deletion software the day after he missed a deposition due to an alleged sickness; (b) Herring's failed attempt to delete approximately 2,500 e-mails pertaining to Plaintiff during the pendency of this lawsuit; (c) Herring's use of a secret/secure e-mail account specifically to avoid disclosure/production in this lawsuit; (d) Herring's commission of perjury when he lied under oath about that secret/secure e-mail account; and (e) Herring's willful destruction of a laptop hard drive which contained years of highly-relevant documents.

[DE 120 at 1]. NITV supports its motion with citation to documentary evidence as well as the sworn declarations of (1) Matt Vanderhoff (Defendants' former longtime Information Technology ("IT") consultant) [DE 103-4]; (2) Andrew Reismann (an expert in digital

forensic, cybersecurity, and information technology services, with a focus on serving the legal industry) [DE 103-2]; and (3) Igor Sestanj (a data recovery engineer) [DE 103-11].

Mr. Herring opposes the motion, claiming "[n]o foul, no harm" regarding his rescheduled deposition, asserting that his former IT consultant was "forced to sign a fake document" under threat of being sued, contending that "[f]ile deletion software is legal to buy and use . . . to free up hard drive space," and arguing that NITV's attorneys are unethical [DE 119 at 7-8, DE 126 at 2-4]. Mr. Herring further contends that he did not act in bad faith or with the intent to deprive NITV of discoverable information.

II. THE LAW OF SPOLIATION

"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). "Sanctions for spoliation of the evidence 'are intended to prevent unfair prejudice to litigants and to ensure the integrity of the discovery process.'" *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F. Supp. 2d 1317, 1323 (S.D. Fla. 2010) (quoting *Flury v. Daimler Chrysler Corp.*, 427 F.3d 939, 944 (11th Cir. 2005)).

Federal Rule of Civil Procedure 37(e) governs claims of spoliation of electronically stored information ("ESI"). *Title Capital Mgmt., LLC v. Progress Residential, LLC*, No. 16-21882-Civ-Williams/Torres, 2017 WL 5953428, at *3 (S.D. Fla. Sept. 29, 2017); *Living Color Enterprises, Inc. v. New Era Aquaculture, Ltd.*, No. 14-62216-Civ-Marra/Matthewman, 2016 WL 1105297, at *3, 4 n.2 (S.D. Fla. Mar. 22, 2016) ("[W]hen confronting a spoliation claim in an ESI case, a court must first look to newly amended

Rule 37(e) and disregard prior spoliation case law based on 'inherent authority' which conflicts with the standards established in Rule 37(e).").

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).

Before imposing sanctions under Rule 37(e), a court must find that: "(1) the information sought constitutes ESI; (2) the ESI should have been preserved in anticipation of litigation; (3) the ESI is lost because a party failed to take reasonable steps to preserve it; and (4) the ESI cannot be restored or replaced through additional discovery." *Title Capital Mgmt.*, 2017 WL 5953428, at *3. If these four threshold requirements are met, sanctions may be warranted if the Court finds prejudice or that the spoliating party acted with the intent to deprive the moving party of the ESI. *Id.* Rule 37(e) gives courts discretion to determine how best to assess prejudice. *Id.* at *6. The intent to deprive standard "may very well be harmonious with the 'bad faith' standard previously established by the Eleventh Circuit" in spoliation cases. *Living Color*, 2016 WL 1105297, at *6 n.6. That is, where there is no direct evidence of bad intent, bad faith may be found on

circumstantial evidence where: "(1) evidence once existed that could fairly be supposed to have been material to the proof or defense of a claim at issue in the case; (2) the spoliating party engaged in an affirmative act causing the evidence to be lost; (3) the spoliating party did so while it knew or should have known of its duty to preserve the evidence; and (4) the affirmative act causing the loss cannot be credibly explained as not involving bad faith by the reason proffered by the spoliator." *See Managed Care Sols., Inc. v. Essent Healthcare, Inc.*, 736 F. Supp. 2d 1317, 1322-23 (S.D. Fla. 2010) (declining to find bad faith and denying a request for an adverse inference instruction); *Calixto v. Watson Bowman Acme Corp.*, 2009 WL 3823390, at *16 (S.D. Fla. Nov. 16, 2009) (declining to find bad faith and denying a request for spoliation sanctions); *Alabama Aircraft Indus., Inc. v. Boeing Co.*, 319 F.R.D. 730, 746 (N.D. Ala. 2017) (finding sufficient circumstantial evidence to conclude that the spoliating party intended to destroy ESI, warranting an adverse inference instruction and an award of attorney's fees and costs).

III. DISCUSSION

To determine whether to impose sanctions in this case, the Court has considered all the evidence presented and the parties' arguments. Upon careful review, the Court finds that the requested sanction of default is warranted.

A. Rule 37(e)'s Four Requirements are Met

First, the information sought by NITV includes emails, email account information, and data stored on various electronic devices. This information constitutes ESI. Second, Mr. Herring knew that the ESI should have been preserved for litigation. To be sure, on February 8, 2019, , the Court issued an Order on Forensic Analysis Protocols [DE 65], which set forth detailed agreed-upon procedures for the collection and forensic review of

electronic data from Defendants' storage media "including but not limited to any laptops, desktops, hard drives, flash drives, servers, networks, or web-based accounts." Under the agreed-upon protocol, a designated independent digital forensic expert would review storage media belonging to Defendants to identify relevant data and data usage information after which Defendants could designate any such information as being privileged. Mr. Herring was aware of this protocol and the requirement that he preserve the designated ESI on behalf of himself and his company. Thus, Rule 37(e)'s first two threshold requirements are met.

Turning to the third requirement, the Court must determine if the ESI was lost because Mr. Herring failed to take reasonable steps to preserve it. The answer is yes. Unrefuted record evidence establishes the following five categories of unreasonable misconduct by Mr. Herring involving the exchange of discovery in this lawsuit.

The first category involves the installation of a "file shredding" program with the intention of deleting files beyond recovery. In this regard, it is undisputed that Mr. Herring was scheduled to appear for a deposition on October 17, 2018 to answer questions on various topics, including:

> 1. The facts and circumstances surrounding the "hard drive crash[]from a computer virus" as alleged by your responses to Plaintiff's jurisdictional discovery requests.
> 2. The software and hardware systems (including but not limited to the name and location of such systems) used by you to store e-mail and other electronic documents.
> 3. Your efforts to recover e-mail and other electronic documents responsive to Plaintiff's jurisdictional discovery requests.

[DE 103-1, Notice of Taking Corp. Rep. Depo., dated 10/15/18]. At the request of Defendants' prior counsel, the deposition was rescheduled on grounds that Mr. Herring was sick and therefore could not attend the deposition [DE 34 at 1]. Notably, however, a

later review of Defendants' laptop hard drives by digital forensic expert Andrew Reisman revealed that on the day after the cancelled deposition, "on October 18, 2018 at 11:46 a.m. eastern, a Google search for 'file shredder filehippo' was performed . . . and a minute later another Google search was run for 'file shredder download…'" [DE 103-2, Reisman Dec. ¶ 4, dated 6/5/19]. One minute later, "[t]he File Shredder setup program 'file_shredder_setup.exe' then was downloaded at 11:47 a.m. eastern that day" and "a program called 'File Shredder' was downloaded to the hard drive from http://www.fileshredder.org/files/" [*Id.*]. According to its website, File Shredder is a "free desktop application for shredding (destroying) unwanted files beyond recovery." *See* Free File Shredder, http://www.fileshredder.org/ (last accessed on 9/18/19). On 6:43 P.M. that same day, Mr. Herring sent an email to his IT consultant, Matt Vanderhoff, stating: "Thanks for the computer work." [DE 103-3].

The digital forensic expert could not determine whether and to what extent files were destroyed using the "file shredder" program [DE 103-2, Reisman Dec. ¶ 5, dated 6/5/19]. However, the sworn declaration of Defendants' former longtime IT consultant Matt Vanderhoff sheds light on this issue. According to Mr. Vanderhoff, "[d]uring the course of this lawsuit, Mr. Herring has asked me on multiple occasions about file deletion software that could be used to permanently delete files that Mr. Herring did not want NITV obtaining access to" [DE 103-4, Vanderhoff Dec. ¶ 8, dated 6/5/19]. Considering the totality of this unrefuted evidence, the Court concludes that Mr. Herring actively pursued and participated in the intentional shredding or attempted shredding of relevant electronic files.

The second misconduct category involves deleting or attempting to delete emails during the pendency of this lawsuit. According to the digital forensic expert, approximately 2,500 emails sent between June 15, 2018 and February 13, 2019 were moved to the "Trash" folder "for deletion but had not yet permanently been deleted from the system" of one of Defendants' laptops [DE 103-2, Reisman Dec. ¶ 8, dated 6/5/19]. In addition, over 2,100 "email fragments dated between June 15, 2018 and February 13, 2019 . . . contained search hits for potentially relevant data" which is an indicator for "when emails are deleted and [are] no longer are recoverable from the Trash folder" [*Id.*]. NITV has provided copies of the recovered emails and a spreadsheet identifying the recovered emails from this timeframe [DE 103-5].

This lawsuit commenced on July 27, 2018 and the parties were actively engaged in discovery thereafter through at least mid-March 2019. The Court's review of the recovered emails provided by NITV reveals that they contain relevant information of evidentiary value in this case. These emails were sent during the pendency of this lawsuit when Mr. Herring had a duty to preserve relevant documents and after the Court ordered him to produce such documents to NITV in discovery [DE 65, DE 76, DE 86]. Instead, Mr. Herring apparently chose to delete or attempt to delete this information.

The third misconduct category involves the use of an undisclosed email address for the purpose of evading discovery. On July 30, 2018, the Monday immediately after this lawsuit was filed, Mr. Herring received an email from a "Jill olson" at jill.olson@gmx.com stating that "it might be a good idea to get a different EMAIL address to communicate with key people to include me" [DE 103-7]. The sender states that "PROTON EMAIL is a good

choice" and that Mr. Herring "will want to DELETE ALL OF THE EMAILS BETWEEN US once you read them as NITV lawyers will be going after your email accounts" [*Id.*].

Around three weeks later, on August 18, 2018, Mr. Vanderhoff avers that Mr. Herring said he had "signed up to proton mail" and "sent a test back to myself and it works fine." [DE 103-8]. Mr. Herring asked Mr. Vanderhoff about secure/encrypted e-mail that "[Mr. Herring] could use to avoid NITV discovering his communications with various parties" [DE 103-4, Vanderhoff Dec. ¶ 7, dated 6/5/19]. Acting against Mr. Vanderhoff's advice that the use of secret emails "was not a good idea," Mr. Herring signed up for the secure/encrypted email address of melody2013@protonmail.com in August 2018 and thereafter sent Mr. Vanderhoff "numerous e-mails concerning NITV and/or the websites at issue in this lawsuit using this melody2013@protonmail.com e-mail address." [*Id.*].

Mr. Herring was deposed on October 24, 2018. During his deposition, NITV's counsel confirmed Dektor's known email address of admin@dektorpse.com and asked Mr. Herring to identify any other email addresses used by Mr. Herring [DE 103-9, Herring Tr. 23:16 – 24:19]. Mr. Herring objected at first but ultimately testified that "[t]he only email address I have for Dektor is admin@dektorpse.com." [*Id.* at 25:15-26:24]. Only after being further pressed by NITV's counsel did Mr. Herring identify one other email address he used, that is Ed@Detectornews.com [*Id.* at 32:7-32:14]. NITV's counsel asked "Are there any other email addresses that you use?" to which Mr. Herring responded "Nope." [*Id.* at 32:15-32:17].

At best, Mr. Herring forgot about the melody2013@protonmail.com address when asked. At worst, he lied under oath—otherwise known as the federal criminal offense of perjury. *See* 18 U.S.C. § 1621. One thing is clear. As evidenced by Mr. Vanderhoff's

declaration and the "Jill olson" email, Mr. Herring knowingly created and used the undisclosed protonmail.com address to participate in unknown communications about NITV and this lawsuit. It is highly doubtful that Mr. Herring forgot he had created that email in July/August when he testified in October.

The fourth category of misconduct involves the circumstances regarding a hard drive that Mr. Herring claimed was damaged. At his October 24, 2018 deposition, Mr. Herring testified regarding a hard drive crash that he said happened in May 2018 and was interfering with his ability to produce responsive documents in discovery:

> **A.** Well, as everybody knows, viruses are very rampant, and I do get virus warnings from my antivirus software from time to time. And one day, I did get a virus warning, and in the next day or two the computer was unable to be used. And I just assumed it was the virus. Upon later discussion with my IT person, he told me the hard drive simply stopped working, it crashed.
> **Q.** You said one day this happened. When did it happen?
> **A.** I think it happened around the middle of May or so.

[DE 103-9, Herring Tr. 8:5 – 9:3].

Contrary to Mr. Herring's testimony about this unexpected hard drive crash, NITV has produced an email suggesting a far more sinister ploy orchestrated by Mr. Herring to deceive NITV with regard to the hard drive. Specifically, on October 9, 2018, Mr. Herring sent Mr. Vanderhoff the following email: "Hi Matt, About middle of [J]une 2018 is better as to when the hard drive became contaminated and useless to use. That would be about 45 days before they filed the suit." [DE 103-10].

Thereafter, on January 7, 2019, the Court ordered Defendants to "cooperate with and allow Plaintiff to conduct a forensic examination and imaging of Defendants' storage media . . . and networked e-mail accounts for documents (existing and/or deleted) relevant to the claims and defenses in this matter" [DE 55 at 2]. On February 8, 2019, the Court

issued its Order on Forensic Analysis Protocols setting forth the parties' agreed-upon data collection and review forensic protocols [DE 65]. During a status conference on February 15, 2019, NITV's counsel advised the Court of a discovery dispute involving a "damaged hard drive located in Pennsylvania" [DE 70]. At the time, Mr. Herring "assure[d the] Court that he has no intention of taking possession of the damaged hard drive prior to the forensics examination." [*Id.*].

Mr. Herring thereafter opposed having his "damaged" hard drive shipped from Pennsylvania to Florida for forensic review. Ultimately, after considering the parties' respective position statements on the matter, the Court ordered that the hard drive be delivered "from the IT safe in Pennsylvania to Orlando for review" in accordance with the Court's Order on Forensic Analysis Protocols [DE 76].

The data recovery engineer who later analyzed the damaged drive avers that:

> In my professional opinion, the above-described damage to the hard drive platter is not indicative of just mechanical failure. Rather, it appears some damage . . . was likely caused by human interference with the hard drive when its cover-lid was removed . . . Unfortunately, no data could be recovered.

[DE 103-11, Sestanj Dec. ¶ 10-12, dated 6/3/19]. This analysis is consistent with Mr. Vanderhoff's sworn statements regarding the supposed hard drive crash. Upon Mr. Herring's request, Mr. Vanderhoff replaced Mr. Herring's laptop hard drive in May 2018 and gave the prior drive back to Mr. Herring "in the event he wanted to extract data" from the drive [DE 103-4, Vanderhoff Dec. ¶ 5, dated 6/5/19]. After Mr. Herring was served with this lawsuit ("at some point in August 2018"), Mr. Herring brought the removed hard drive back to Mr. Vanderhoff and asked Mr. Vanderhoff to store the hard drive in his safe [*Id.*]. Mr. Vanderhoff noticed that "the drive's encasement had been opened and that the

drive may have been physically damaged." Even more troubling, Mr. Herring apparently told Mr. Vanderhoff at that time to tell anyone who asked that the hard drive was in Mr. Vanderhoff's possession from May 2018 through that date "rather than the truth which was that Herring had the hard drive for that period of time" [*Id.*].

The data recovery engineer and the digital forensics expert both agree that the formatting of the subject drive is not consistent with mechanical failure or a computer virus; rather, the "most likely explanation for this is that someone formatted the hard drive (prior to the above-referenced physical damage) by 'zero-filling' the drive—a method of formatting a hard drive whereby the formatter wipes the contents by overwriting them with zeros" [DE 103-11, Sestanj Dec. ¶ 13-14, dated 6/3/19; DE 103-2, Reisman Dec. ¶ 7, dated 6/5/19 (agreeing with Mr. Sestanj's opinion "that deliberate human interference is the explanation for the data on the Damaged Drive being inaccessible"].

As conveyed by Mr. Vanderhoff, while this lawsuit was pending, Mr. Herring reached out to ask "whether he could purchase a new hard drive at Walmart that could be 'swapped' for his existing hard drive in the event that a further forensic examination of the hard drive was ordered" [DE 103-4, Vanderhoff Dec. ¶ 8, dated 6/5/19]. Mr. Vanderhoff understood this to mean "Mr. Herring wanted to provide a 'dummy' drive devoid of data to the forensic expert so he could avoid disclosure of his actual files/documents" [Id.]. Mr. Herring has not offered any argument or evidence to refute Mr. Vanderhoff's declaration about the hard drive or otherwise.

The fifth and final category of misconduct involves Mr. Herring's apparent intention to defy this Court's orders. On May 17, 2019, the Court issued a detailed Order [DE 95] granting final default judgment as to liability only against Dektor Corporation and

issuing a permanent injunction which mandated, among other things, the immediate takedown of the www.NITVCVSAexposed.com website. Upon learning of the Court's Order, Mr. Vanderhoff (as the website's host) took the website offline [DE 103-4, Vanderhoff Dec. ¶ 10, dated 6/5/19]. Mr. Herring was "displeased" and asked Mr. Vanderhoff about hosting the website "offshore so that it would be beyond the reach of any court in the United States." [*Id.*]. Mr. Vanderhoff "told Mr. Herring that I would not assist him with doing that, but he indicated that is the course he is pursuing at this time." [*Id.*].

Confronted with the evidentiary submissions detailed above, Mr. Herring's reply is largely non-responsive. Mr. Herring's arguments focus on his views about the overall merits of this case as opposed to offering a response to the misconduct alleged by NITV. In conclusory fashion, Mr. Herring contends that "Nitv/lawyers demanded a hard drive examination under false pretenses." [DE 119 at 8]. It is unclear how so. Mr. Herring also suggests that Mr. Vanderhoff was forced "to sign a fake document." [DE 126 at 3]. Yet, Mr. Herring offers no evidentiary proof in support of this statement.

Mr. Herring also argues that "file deletion software is legal to buy and use . . . to free up hard drive space" [*Id.* at 2]. This argument misses the point, which is that Mr. Herring was under an affirmative obligation to preserve his files during the pendency of this suit. Mr. Herring takes issue with NITV's statements about Mr. Herring's actions or responses since "[a] business (law) that is written in a foreign language (legalese) and forms written in legalese CANNOT be stated by lawyers that non-trained people sould be able to understand those rules and forms." [DE 126 at 3]. That Mr. Herring has chosen to proceed *pro se* in this matter cannot be used as a shield protecting him from his discovery obligations or the imposition of sanctions based on deliberate misconduct. The Court finds

that Mr. Herring was fully aware of his obligations as a litigant in this suit and his explanations for deleting or losing relevant ESI demonstrate an unreasonable failure to preserve.

Mr. Herring knew that ESI including his emails and electronic storage devices had to be preserved for forensic review in this litigation and he acted unreasonably in deleting ESI, attempting to delete ESI, or using an undisclosed email address to avoid the ESI from being reviewed. The agreed-upon forensic protocol provided a process for determining the relevance of captured ESI. It was not for Mr. Herring to unilaterally decide what might or might not be relevant. All of the foregoing establishes that Rule 37(e)'s third threshold requirement—*i.e.* that the ESI is lost because a party failed to take reasonable steps to preserve it—is satisfied.

The fourth requirement is also met. The sworn declarations of the digital forensic expert and the data recovery engineer together with Mr. Vanderhoff's declaration establish that certain emails and data were intentionally removed with Mr. Herring's knowledge and at his direction from Defendant's electronic devices and email accounts beyond recovery. While NITV could conceivably attempt to piece together the larger puzzle of what might have been on Mr. Herring's devices or in his email accounts through other sources, NITV can never know for sure without the ability to properly analyze these ESI sources. This is precisely why the parties entered the stipulated forensic review process in the first place.

B. Prejudice and Intent to Deprive

Having found that Rule 37(e)'s four threshold requirements are met, the Court must next determine if NITV is prejudiced as a result of the lost ESI and/or if Mr. Herring acted with the requisite intent to deprive NITV of the ESI at issue. Yes to both inquiries. As for

prejudice, without the ability to conduct a fair forensic review the devices belonging to Defendants or the emails in all of Mr. Herring's email accounts from the relevant timeframe, NITV has lost key evidence regarding whether and to what extent, if at all, Mr. Herring competed unfairly, tortiously interfered, defamed, or disparaged NITV and NITV's product. Such evidence goes to the heart of NITV's alleged claims in this case. For instance, NITV alleges that Mr. Herring has engaged in an unrelenting campaign of harassment against NITV by sending emails to law enforcement agencies nationwide containing false information about NITV and NITV's product. Without access to the lost or destroyed emails and other related ESI for forensic review, this claim cannot be readily analyzed during a full and fair trial on the merits.

As for intent, the Court finds that the evidence present sufficiently establishes that Mr. Herring acted with the intent to deprive NITV of the ESI and interfere with NITV's ability to discover discoverable information. First, the ESI located in Mr. Herring's email accounts and on his electronic devices "could fairly be supposed to have been material to the proof or defense of a claim at issue in the case." *Managed Care Sols.*, 736 F. Supp. 2d at 1323. As demonstrated by several emails produced by third parties, Mr. Herring was communicating via email with others regarding issues in this case. Without access to the emails in all of Mr. Herring's accounts, NITV is unable to determine the full scope of Mr. Herring's communications and activities during the relevant timeframe. Similarly, NITV is unable to trace the history of the electronic data while it was in Mr. Herring's possession.

Second, through his affirmative actions, Mr. Herring intentionally caused the ESI to be damaged or lost beyond recovery. This is shown through Mr. Vanderhoff's declaration. Third, Mr. Herring did so at a time that he had counsel and after having been

duly advised of the stipulated forensic review process—illustrating that he knew or should have known that he was obligated to take precautions to preserve relevant ESI in his email accounts and electronic devices. Considering the totality of the circumstances—including but not limited to the installation of a file shredder program around the time of a scheduled deposition, Mr. Herring's statements to his former IT professional demonstrating his continuing efforts to obstruct the forensic review process, and the sworn declarations of an independent digital forensic expert and data recovery engineer regarding their review of available electronic devices belonging to Mr. Herring—the Court concludes that Mr. Herring did not safeguard or preserve his ESI as required. On the contrary, Mr. Herring's affirmative actions caused the loss or destruction of the ESI and "cannot be credibly explained as not involving bad faith by the reason[s] proffered." *See Managed Care Sols.*, 736 F. Supp. 2d at 1323.

C. Sanctions

As sanctions, NITV proposes a Court Order entering a default against Mr. Herring and directing NITV to proceed with a motion for final default final judgment against Mr. Herring [DE 103 at 17]. In its discretion, and after careful consideration, the Court finds this proposal to be an appropriate measure in this case. *See Eagle Hosp. Physicians, LLC v. SRG Consulting, Inc.*, 561 F.3d 1298, 1306 (11th Cir. 2009) (default judgment is an appropriate sanction only when less drastic measures are insufficient). Our society and our legal system both depend upon the fundamental truthful conduct of persons. When that truthfulness is compromised or absent, the processes still work, but not nearly as well. In those situations, Courts have the authority to impose sanctions to penalize those who damage the operations of our valuable judicial process. Sometimes the misconduct is so

pervasive and impactful that normal sanctions are not enough because then the process does not work. The extraordinary sanction becomes appropriate in such an extraordinary circumstance. Such is the case here.

IV. CONCLUSION

Based on the foregoing, the Court concludes that the evidentiary submissions demonstrate that Mr. Herring affirmatively acted on various occasions with the intent to deprive NITV of discoverable ESI and other information. The Court further finds that NITV suffered prejudice by this loss, such that sanctions are warranted. Mr. Herring's extraordinary misconduct warrants the imposition of the extraordinary sanction of default.

Accordingly, the Court **ORDERS AND ADJUDGES** that Plaintiff's Motion for Sanctions Against Herring for Spoliation of Evidence and Discovery Abuse [DE 103] is **GRANTED**. Within 21 days of this Order, NITV shall file an appropriate motion for final default judgment against Mr. Herring. Such motion shall be accompanied by a proposed order that is filed and submitted via e-mail to the Court at brannon@flsd.uscourts.gov. *See* S.D. Fla. Local Rule 7.1(a)(2). NITV's motion may include information regarding the final amount of monetary damages to be imposed against both Defendants. In this regard, NITV shall heed the Court's prior statements regarding the need to file satisfactory evidentiary submissions in support of any request for financial damages.

DONE AND ORDERED in Chambers at West Palm Beach in the Southern District of Florida, this 20th day of September, 2019.

DAVE LEE BRANNON
U.S. MAGISTRATE JUDGE