IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IHS GLOBAL LIMITED and IHS GLOBAL, INC.,	)	
Plaintiffs,	)	No. 2:18-cv-01025-DCN
vs.	)	**ORDER**
TRADE DATA MONITOR LLC, C. DONALD BRASHER, JR., KRISTEN STEIN, and BRIGITTE STRINGFIELD,	)	
Defendants.	)	

The following matter is before the court on plaintiffs IHS Global Limited and IHS Global, Inc's (collectively, "plaintiffs") motion to compel, ECF No. 117. For the reasons set forth below, the court grants the motion.

I. BACKGROUND

This case arises out of a variety of disputes between two competing companies. Plaintiffs own and operate a database called Global Trade Atlas ("GTA"). GTA provides comprehensive merchandise trade statistics, including monthly import and export data for more than 95 countries and annual import and export data for more than 180 countries. Defendant C. Donald Brasher, Jr. ("Brasher") and his brother created GTA through their company, Global Trade Information Services, Inc. ("GTIS"). On August 1, 2014, plaintiffs acquired GTIS, including GTA, through a Stock Purchase Agreement ("SPA"). Under the SPA, Brasher and his affiliates were prohibited from using any confidential or proprietary information related to GTIS, including GTA, for three years—until August 1, 2017— and "until such information can no longer be reasonably considered to be a Trade

Secret." ECF No. 25 ¶ 22. The SPA defines "Trade Secret" as "confidential and proprietary information, including trade secrets, know-how, processes, schematics, business methods, formulae, drawings, prototypes, models, designs, databases, customer lists and supplier lists." Id.

After selling GTIS to plaintiffs, Brasher worked as a consultant for plaintiffs. Pursuant to this arrangement, Brasher entered into a consulting agreement ("Consulting Agreement") where he promised not to use plaintiffs' confidential and proprietary information. Plaintiffs allege that while working both for GTIS and for plaintiffs, Brasher had "extensive access to and knowledge of GTIS's and now [plaintiffs'] trade secrets." Id. ¶ 36. Plaintiffs also allege that Brasher had access to this information on his laptop, which he used during his time at GTIS and retained after his consulting period ended in May 2015.

Plaintiffs allege that soon after Brasher stopped working as a consultant for plaintiffs, he began to work on the Trade Data Monitor Product ("TDM Product"), a "copycat version" of the GTA product. Id. ¶ 45. Plaintiffs allege that defendant Trade Data Monitor LLC ("TDM") was formed by Brasher on May 2, 2016 as ANH Enterprises LLC, although today it is known as TDM. Plaintiffs then allege that in November and December 2016, TDM filed trademarks for "TRADE DATA MONITOR" and "TDM," both of which are described as providing search engines for global import and export data. According to the amended complaint, Brasher and TDM began contacting suppliers around mid-2016 to obtain data for the TDM Product and began to develop the TDM Product around October 2016. Then, plaintiffs allege, Brasher launched the TDM

Product around August 1, 2017, the day after Brasher's non-competition agreement expired.

Plaintiffs allege that defendants used plaintiffs' product, supplier, and customer trade secrets to create the TDM Product. In addition, plaintiffs allege that defendants have been using plaintiffs' confidential customer information, including contact information, pricing arrangements, and subscription preferences, to create business for TDM. In particular, plaintiffs allege that defendants used plaintiffs' trade secrets about when plaintiffs' customers' subscriptions to GTA were up for renewal in order to strategically and timely solicit plaintiffs' customers.

Plaintiffs filed this case on April 16, 2018. The operative complaint is plaintiffs' amended complaint, which alleges various breaches of contracts between the parties, a violation of The Defend Trade Secrets Act, a violation of the Uniform Trade Secrets Act of Colorado and South Carolina, and several tort claims. On November 27, 2019, plaintiffs filed a motion to compel the forensic inspection of Brasher's laptop. ECF No. 117. Defendants responded to the motion on December 11, 2019, ECF No. 126, and plaintiffs filed a reply on December 17, 2019, ECF No. 127. The court held a hearing on the motion on December 19, 2019.

II. STANDARD

Pretrial discovery is governed by Rule 26 of the Federal Rules of Civil Procedure. Parties are permitted to "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). In determining proportionality, a court should consider "the importance of the issues at stake in the action, the amount in controversy, the parties'

relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Id. When a party fails to respond to a discovery request or responds in an incomplete manner, the party seeking discovery may file a motion to compel discovery responses. Fed. R. Civ. P. 37(a)(3)(B); Fed. R. Civ. P. 37(a)(4).

III. DISCUSSION

Plaintiffs ask the court to compel a forensic inspection of Brasher's laptop. Brasher used his laptop while working for both plaintiffs and TDM, and plaintiffs allege that Brasher misused plaintiffs' proprietary information that he accessed on his laptop. During the course of discovery, Brasher has produced documents from his laptop, some of which include information about plaintiffs' customer history and contact information. The parties disagree about whether this information is properly classified as "trade secrets," but plaintiffs contend that the information produced includes their proprietary information and trade secrets. Now plaintiffs want to conduct a forensic inspection of the laptop to see what documents are and previously were on the laptop as well as how and when Brasher and others accessed, modified, copied, or used those documents. Plaintiffs argue that this request will impose a minimal burden on defendants because defendants have already made a forensically sound image of the laptop, and that defendants can just allow plaintiffs' forensic imager to inspect and make a copy of the forensic image.

Defendants[1] respond by arguing that the request is overbroad and seeks irrelevant and potentially privileged material. Defendants argue that plaintiffs have failed to set forth sufficient reasoning for the extraordinary request of a forensic image. They explain that they have already produced the responsive and nonprivileged documents from Brasher's laptop, and that absent any claim of wrongdoing, a forensic image of the laptop is not warranted. Defendants also argue that plaintiffs' request is untimely because defendants have always been clear that they only intended to produce responsive documents from the laptop and yet plaintiffs are just now requesting a forensic inspection after discovery has been ongoing for over a year.

The court addresses defendants' timeliness argument first. Pursuant to Local Rule 37, motions to compel discovery must be filed within 21 days after receipt of the discovery responses to which the party challenges. Local Civ. Rule 37.01 (D.S.C.). Defendants responded to plaintiffs' request for a forensic inspection on November 22, 2019. Plaintiffs filed their motion to compel five days later. Therefore, plaintiffs' motion is timely, and the court can consider it. To the extent that defendants argue that the motion is untimely because plaintiffs waited over a year into discovery to request a forensic inspection, that argument is unconvincing. Discovery is still ongoing, with fact discovery set to end on March 30, 2020 and expert discovery set to end on April 30, 2020. Plaintiffs are entitled to make discovery requests at any point during discovery.

[1] Plaintiffs' motion is directed at all defendants; therefore, the court will refer to all defendants. However, plaintiffs do not argue or even suggest that Brasher's laptop is within the possession, custody, or control of defendant TDM, defendant Kristen Stein, or defendant Brigitte Stringfield.

Having found plaintiffs' motion to be timely, the court now turns to the substance of the motion. Plaintiffs want to inspect and copy the forensic image of Brasher's laptop, which "is generally described as a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." Balboa Threadworks, Inc. v. Stucky, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006) (internal quotation omitted). Rule 34 permits a party to make a request during discovery to inspect electronically stored information ("ESI"). Fed. R. Civ. P. 34(a). The Advisory Committee Notes scale back the scope of this general rule:

> Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Advisory Committee Notes to Fed. R. Civ. P. 34. Rule 26 also places specific limitations on the production of ESI, providing that "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." Fed. R. Civ. P. 26(b)(2)(B). If the party shows that the ESI is not reasonably accessible, "the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C)." Id. Those limitations require the court to limit the extent of discovery if "the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;" if "the party seeking discovery has had ample opportunity to obtain the information by discovery in the action;" or if the discovery is outside of the general scope

of discovery, i.e., not relevant to a party's claim or defense or not proportional to the needs of the case. Fed. R. Civ. P. 26(b)(2)(C).

"[F]orensic imaging is not uncommon in the course of civil discovery." John B. v. Goetz, 531 F.3d 448, 459 (6th Cir. 2008). In cases "where trade secrets and electronic evidence are both involved, the Courts have granted permission to obtain mirror images of the computer equipment which may contain electronic data related to the alleged violation." Balboa Threadworks, Inc, 2006 WL 763668, at *3; Physicians Interactive v. Lathian Sys., Inc., 2003 WL 23018270, at *10 (E.D. Va. Dec. 5, 2003). "On the other hand, Courts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature." Balboa Threadworks, Inc., 2006 WL 763668, at *3. "[M]ere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures." Goetz, 531 F.3d at 460. As such, "even if acceptable as a means to preserve electronic evidence, compelled forensic imaging is not appropriate in all cases, and courts must consider the significant interests implicated by forensic imaging before ordering such procedures." Id. In considering these interests, "the degree to which the proposed inspection will aid in the search for truth must be balanced against the burdens and dangers created by the inspection." Belcher v. Bassett Furniture Indus., Inc., 588 F.2d 904, 908 (4th Cir. 1978).

Applying the framework created by Rules 26 and 34, the court finds that plaintiffs are entitled to inspect and copy the forensic image of Brasher's laptop. First, the court is unconvinced that a forensic image of Brasher's laptop is not reasonably accessible.

Defendants have already made a forensic image of the laptop. Defendants argue that the forensic image contains nonresponsive and privileged documents, and that because defendants have already reviewed the documents on the laptop for responsiveness and privilege, it would be burdensome to require defendants to go back and conduct another review of the forensic image. However, as discussed in greater detail below, the court will appoint an expert witness to conduct the inspection and make the copy of the forensic image, and the court is confident that the parties can agree upon a protocol to ensure that the expert can efficiently identify the non-privileged and responsive material.

Moreover, even if a forensic image of the laptop were not reasonably accessible, good cause exists for the production of the forensic image. As part of plaintiffs' trade secret claim, they must show that defendants used and misappropriated their trade secrets. See Nucor Corp. v. Bell, 482 F. Supp. 2d 714, 725 (D.S.C. 2007). Defendants' production of documents from Brasher's laptop have established that plaintiffs' allegedly proprietary and confidential information was stored on the laptop. However, because Brasher used the laptop when he worked as a consultant for plaintiffs, the existence of the information on his laptop alone is insufficient to show misuse. The relevant inquiry is whether Brasher accessed that information and the extent to which he used it after he stopped working for plaintiffs, and that is what plaintiffs seek to discover from obtaining a forensic image of the laptop. For this reason, the connection between the laptop and the claims in this suit is not "unduly vague or unsubstantiated in nature." Balboa Threadworks, Inc., 2006 WL 763668, at *3. Indeed, "allegations that a defendant downloaded trade secrets onto a computer provide a sufficient nexus between plaintiff's claims and the need to obtain a mirror image of the computer's hard drive." Ameriwood

Indus., Inc. v. Liberman, 2006 WL 3825291, at *4 (E.D. Mo. Dec. 27, 2006), as amended on clarification, 2007 WL 685623 (E.D. Mo. Feb. 23, 2007). Here, the nexus is even stronger because plaintiffs don't simply allege that defendants downloaded the alleged trade secrets—defendants have produced documents from Brasher's laptop that contain the alleged trade secrets. Therefore, there is good cause for discovery of the forensic image, and the forensic image is both relevant to plaintiffs' trade secret claim and proportional to the needs of the case.

Defendants, citing to several cases, argue that courts generally order a forensic inspection or mirror image of a computer only when there is some evidence of wrongdoing or suspicious behavior by the party subject to the inspection, making a forensic inspection unwarranted here because plaintiffs have not made a credible assertion of wrongdoing by defendants. However, those cases are inapposite to the current matter because the purpose of forensic inspection in those cases was to determine if the party subject to inspection possessed the trade secrets at issue despite their claims otherwise. See Ameriwood Indus., Inc., 2006 WL 3825291, at *3 (ordering forensic inspection of a laptop after defendants represented that they already produced the requested information because evidence existed that one of the defendants may have deleted emails prior to producing them); Balboa Threadworks, Inc., 2006 WL 763668, at *4 (ordering mirror imaging in part because "[t]he fact that [the defendant] used one of his computers to draft a document that is related to alleged acts of infringement in this case . . . runs contrary to claims that his computers were never used in connection with the embroidery business"); Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc., 2012 WL 70428, at *3 (N.D. Cal. Jan. 9, 2012) (ordering a forensic inspection of one of the

defendants' hard drives after the plaintiff unsuccessfully sought information from the defendants and deposition testimony suggested that the hard drive had been deleted); Koosharem Corp. v. Spec Pers., LLC, 2008 WL 4458864, at *1 (D.S.C. Sept. 29, 2008) (finding forensic inspection of defendants' computers to be warranted because "not a single email produced by the defendants is an accurate copy of the original email, as the date and time stamp on every email has been modified to reflect the dates the emails were compiled rather than the dates they were sent" and because "irregularities exist in the emails that were produced that call into question the authenticity of the documents"). In other words, the wrongdoing or suspicious behavior led these courts to determine that a forensic inspection was warranted to determine if trade secrets were in the parties' possession despite claims otherwise.

In contrast, here defendants have produced documents that show that plaintiffs' allegedly proprietary information and trade secrets were in Brasher's possession via his laptop. Therefore, there is no need for any showing of wrongdoing because there is already evidence that Brasher possessed plaintiffs' information. That alone is evidence of potential wrongdoing that is worth further investigation. The forensic inspection's purpose here is not to resolve a suspicious inconsistency in defendants' productions. Instead, its purpose is to obtain additional information about documents that have already been produced and are clearly relevant to plaintiffs' claims. Plaintiffs' request for a forensic inspection is not based on "mere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures," Goetz, 531 F.3d at 460, but instead is based on evidence of Brasher's possession of alleged trade secrets and the need for further information on the full extent

of the use of those alleged trade secrets. In Ameriwood Indus., Inc., the court acknowledged the relevancy of the type of information plaintiffs seek in trade secret cases by noting that

> other data may provide answers to plaintiff's other pertinent inquiries in the instant action, such as: what happened to the electronic files diverted from plaintiff to defendants' personal email accounts; where were the files sent; did defendants store, access or share the files on any portable media; when were the files last accessed; were the files altered; was any email downloaded or copied onto a machine; and did defendants make any effort to delete electronic files and/or "scrub" the computers at issue.

2006 WL 3825291, at *3. This is precisely the information plaintiffs seek. Based on plaintiffs' counsel's representation at the hearing on the motion, the court is also convinced that plaintiffs do not intend to use a forensic inspection as a method of unfettered access to Brasher's computer and will endeavor to only identify and copy information that is directly relevant to their claims.

Defendants also rely on Cross by & Through Steele v. XPO Express, Inc. to show that courts are generally hesitant to order a forensic examination or inspection of a laptop absent any showing of wrongdoing. See 2016 WL 11519221, at *7 (D.S.C. May 3, 2016) (finding a forensic examination of a laptop to be unwarranted because "[u]nlike in other cases where forensic examinations have been ordered, there is no evidence here that [defendants]' laptop has crashed or been wiped clean"). However, in that case, the plaintiff sought to conduct a forensic examination of the defendant's personal laptop simply to look for "any communication messages, documents, programs, and/or any other information and/or documents on [the] laptop that will shed light on [the defendant]'s relationship with [the other defendants]." Id. at *6. The court concluded that this goal could be achieved by ordering the defendant to conduct a search of his laptop for responsive documents, making a forensic examination unnecessary and unwarranted.

Here, plaintiffs do not seek a forensic inspection of Brasher's laptop simply to find documents that could be produced otherwise. Instead, the purpose of the forensic inspection is to determine when Brasher last accessed and used documents that have already been produced.

In sum, the court grants plaintiffs' motion. To facilitate the inspection and copying of the laptop's forensic image, the court will appoint an expert witness pursuant to Rule 706 of the Federal Rules of Evidence. The expert must be a neutral third-party who has not been engaged by plaintiffs or defendants in this case. The court instructs the parties to confer and agree upon who shall serve as the expert.[2] Pursuant to Rule 706(c), the expert will be entitled to reasonable compensation. The plaintiffs will be responsible for 50% of the expert's compensation, and Brasher will be responsible for the other 50% of the compensation. Per Rule 706(c), the expert's compensation will be charged like other costs.

The court also instructs the parties to confer and agree upon a protocol for the inspection and copying of the forensic image of Brasher's laptop, taking particular care to prevent the disclosure of any privileged or personal, unresponsive information within the forensic image of the laptop. The parties shall file a joint letter by January 20, 2019 that either: (1) identifies the agreed upon expert and protocol; or (2) explains the reason as to why the parties could not come to an agreement and includes each party's proposal for an expert and for the protocol. If the parties cannot agree upon the expert and/or the protocol, the court will consider the information in the parties' joint letter and appoint an

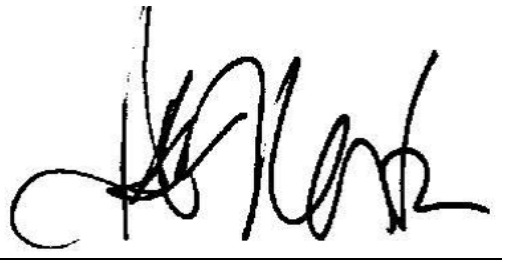
[2] At the hearing on the motion, there was discussion of using John Akerman of Rosen Litigation Technology to facilitate the forensic inspection. The court is amenable to appointing Mr. Akerman if the parties so agree.

expert and/or establish a protocol. Once the court appoints an expert witness and a protocol is established, defendants must make the forensic image of Brasher's laptop available to the expert for inspection and copying in accordance with the established protocol.

IV. CONCLUSION

For the reasons set forth above, the court **GRANTS** the motion.

AND IT IS SO ORDERED.



DAVID C. NORTON
UNITED STATES DISTRICT JUDGE

December 23, 2019
Charleston, South Carolina