IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO

Brandon Hausauer, et al.,	**Case No. 1:20mc101**
Plaintiffs,	
-vs-	**JUDGE PAMELA A. BARKER**
TrustedSec, LLC,	
Defendants	**MEMORANDUM OPINION AND ORDER**

Currently pending is the Motion of Plaintiffs Brandon Hausauer, Caralyn Tada, Emily Behar, Gary Zielicke, Emily Gershen, Whitney Anne Palencia, John Spacek, and Sara Sharp (hereinafter "Plaintiffs") for Transfer, or in the Alternative, to Compel. (Doc. No. 1.) Defendant TrustedSec, LLC filed a Brief in Opposition, to which Plaintiffs responded. (Doc. Nos. 9, 10.) For the following reasons, Plaintiffs' Motion is DENIED.

I. Factual Background

In their filings before the Court, Plaintiffs state the following. On July 19, 2019, Capital One announced a data breach involving the exfiltration of the highly sensitive personal information of over 100 million of its customers. The data was obtained by an outside hacker who was later charged with computer fraud and abuse. Various complaints alleging that Capital One failed to take reasonable care to secure the sensitive information belonging to its customers were filed around the country. The Judicial Panel on Multidistrict Litigation ("MDL") transferred the actions to the Eastern District of Virginia where District Judge Anthony John Trenga and Magistrate Judge John Anderson have presided over the litigation. *See In re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (E.D. Va.)

In the MDL action, Plaintiffs issued eleven (11) Fed. R. Civ. P. 45 subpoenas to third party entities that provided cybersecurity services to Capital One before the breach, that conducted forensic investigations into the causes of the breach, or that analyzed the personal customer data that was exfiltrated. One of these subpoenaed entities is Defendant herein, TrustedSec, LLC, which is located in Strongsville, Ohio. Specifically, on May 21, 2020, Plaintiffs issued a subpoena to TrustedSec pursuant to Rule 45 that sought the production of twenty-two (22) separate categories of documents relating to the cybersecurity services it provided to Capital One, including (but not limited to) documents relating to the following: (1) the scope of services performed by TrustedSec for Capital One, including any master services agreement, statements of work, and Amazon support services; (2) any written reports or other documentation concerning the work TrustedSec provided or proposed to provide in connection with Capital One's computer systems, security, and/or the data breach; (3) the identities of each of TrustedSec's employees who consulted with or provided services to Capital One; (4) communications regarding the data breach, Capital One's data security, or Capital One's security vulnerabilities; (5) Capital One's awareness of vulnerabilities in its computer systems; and (6) penetration testing of Capital One's cybersecurity environments prior to and after the breach. (Doc. No. 1-3, Exh. 1.) TrustedSec agreed to accept service of the subpoena as of June 9, 2020. (Decl. of Christopher Swing (Doc. No. 9-2) at ¶ 3.)

On June 21, 2020, TrustedSec objected to the subpoena on numerous bases, including relevancy, undue burden, and proportionality. (Doc. No. 1-3 at PageID# 63-65.) Counsel for the parties thereafter engaged in discussions to narrow the requests, including narrowing the time frame

for the requested documents.[1] (Swing Decl. at ¶ 6.) In early July 2020, TrustedSec began searching for and assembling responsive documents. (Swing Decl. at ¶ 6; Doc. No. 1-3 at PageID# 78.) On July 23, 2020, TrustedSec produced its master services agreement with Capital One and all of the consulting reports for its work, along with written information relating to (1) the dates that TrustedSec provided network security services to Capital One, including the dates of specific testing; (2) the names of the TrustedSec employees that interacted with Capital One regarding penetration testing services; and (3) the names of the Capital One employees that TrustedSec interacted with regarding penetration testing. (Doc. No. 8-6 at PageID#s 219-229) (filed under seal).

On August 5, 2020, Plaintiffs proposed a list of 34 search terms or phrases for locating potentially relevant electronically stored information ("ESI"). With a few limited exceptions, each of these phrases included iterations of certain words and letters coupled with the phrases "Capital One" or "Cap One."[2] (Swing Decl. at ¶ 8; Doc. No. 9-2 at PageID#s 259-260.) Plaintiffs requested that TrustedSec run the search terms against "sources of potentially relevant documents," including email (both external and internal) and TrustedSec's instant messaging service, MatterMost. (Doc.

[1] Plaintiffs agreed to narrow their request from a five-year period to the period from 2018 to January 2020. (Doc. No. 10 at p. 2, fn 1.)

[2] By way of example, some of the search terms or phrases originally proposed by Plaintiffs include the following: (1) ("Security Information and Event Management" OR SIEM) AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR@capitalone.com); (2) "Cloud Custodian" AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR @capitalone.com); (3) (GuardDuty OR "Guard Duty") AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR@capitalone.com) (4) ((IAM OR "identity and access management" OR "identity management") w/100 permission*) AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR @capitalone.com); (5) ("instance metadata service" OR "IMS") AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR@capitalone.com); (6) (Cyber* AND (budget OR spend*)) AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR@capitalone.com); and (7) (Encrypt* w/10 (data OR "PII" OR "personally-identifiable information" OR "personally identifiable information" OR (customer w/5 (information OR data) OR s3 OR bucket*)) AND ("Capital One" OR CapitalOne" OR "Cap One" OR "CapOne" OR @capitalone.com). (Doc. No. 9-2 at PageID# 259.)

No. 1-3 at PageID# 81.) Plaintiffs also requested that, after running the searches, TrustedSec provide "hit reports for further potential revision of terms." (*Id*.)

TrustedSec agreed to Plaintiffs' proposed search terms but asserts that it did not agree to provide "hit reports." (Swing Decl. at ¶ 8; Doc. No. 1-3 at PageID# 91.) Plaintiffs objected, and argued that the parties should engage in the following process: (1) TrustedSec should first conduct a search based on the original search terms provided by Plaintiffs (2) TrustedSec should then run "hit reports" to determine the accuracy of those original search terms, (3) the parties should then evaluate the results of the "hit reports" and cooperate to develop revised search terms; (4) TrustedSec should then run the revised search terms against its ESI databases; and, finally, (5) TrustedSec should then produce the documents generated as a result of the search using the revised search terms. (Doc. No. 1-3 at PageID# 89.) TrustedSec declined to engage in this process, noting that it had already produced all of the technical consulting reports that it had conducted for Capital One and yet Plaintiffs "have still been unable to point [] to any evidence that TrustedSec provided consulting services pertaining to the compromised system at issue in the subject lawsuit." (*Id*. at PageID# 91.) TrustedSec further indicated that "hit reports" are not the "natural byproduct" of the work commenced by TrustedSec in response to Plaintiffs' subpoena. (*Id*.)

Plaintiffs continued to insist that TrustedSec provide "hit reports," stating as follows: "We renew our request for information on the methods used for searching TrustedSec's ESI sources as well as the hit reports from the initial search terms we proposed. We renew our request to see these hit reports (or whatever TrustedSec's methods return from the proposed search terms) and be provided an opportunity to revise the initial terms as needed." (Doc. No. 1-3 at PageID# 93.) On September 14, 2020, TrustedSec agreed to "provide information regarding the methods used for searching,

together with what TrustedSec's methods return from the proposed search terms." (Doc. No. 1-3 at PageID# 96.)

On September 24, 2020, TrustedSec supplemented its production with its (1) internal email captured by the search terms; (2) all of its external email with Capital One; and (3) correspondence from its instant messaging service, MatterMost. (Swing Decl. at ¶ 9.) In addition, on that same date, TrustedSec confirmed that it "was able to run query reports in an effort to fulfill putative class plaintiffs' counsel's request for 'hit reports.'" (Doc. No. 1-3 at PageID# 103.) TrustedSec provided an excel spreadsheet with numbered worksheets showing the results. (*Id.*) Plaintiffs note that this report shows that 21 of the 33 search terms did not hit on any documents. (Doc. No. 10 at p. 6.)

TrustedSec states that, in total, it produced 1,827 documents containing 9,060 pages, including over 1,500 emails with attachments, "all of which identifies the history, substance and findings of TrustedSec's work for Capital One and the key players involved." (Doc. No. 9 at p. 1.) In an Affidavit attached to its Brief in Opposition, TrustedSec's Chief Executive Officer David Kennedy further states as follows:

> 6. It was requested that TrustedSec recover any data associated with the Capital One engagement, which included a number of different systems including file shares, SharePoint, chat software, electronic mail (e-mail), and databases. In addition, the search criteria was performed over the entire Exchange infrastructure utilizing Office 365 as well as needing to create custom queries through the SQL database through the chat software (MatterMost), which required extensive work in order to decrypt the SQL table structures with the encryption keys and extract the appropriate search terms through the database itself. TrustedSec has provided all related search terms, results, documents, and data related to Capital One.
>
> 7. I am aware that TrustedSec produced the following types of documents and information in response to the plaintiffs' document subpoena:
>
> • The identities of all custodians and sources of TrustedSec's ESI related to Capital One;

> • TrustedSec's master services agreement with Capital One with scope of work, and all of the technical consulting reports prepared by TrustedSec for Capital One reflecting work performed by TrustedSec for Capital One;
>
> • The results of TrustedSec's work and what it reported to Capital One;
>
> • All of TrustedSec's external email correspondence with Capital One; TrustedSec's internal email correspondence returned from the search terms and TrustedSec's instant messaging service, Mattermost, returned from the search terms; and query reports that contain information on the results of running Plaintiffs' search terms against the agreed upon sources and custodians of ESI pertinent to Capital One; and
>
> • The resources Capital One allocated to. and any time constraints Capital One imposed on, TrustedSec's work.

(Declaration of David Kennedy (Doc. No. 9-1) at ¶¶ 6-7.) Mr. Kennedy further states that "[i]t took TrustedSec personnel approximately 63 hours to gather [all of the] information [requested], at an internal cost of approximately $18.900." [3] (*Id.* at ¶ 10.)

On October 12, 2020, Plaintiffs provided a list of revised search terms and requested that TrustedSec return search term results/hit reports for these new terms within two days; i.e., by October 14, 2020. (Doc. No. 1-3 at PageID# 105.) This list of revised search terms contained another 37 search terms or phrases. (Doc. No. 9-2 at PageID#s 262-263.) Most of these revised terms were identical to the previous terms but omitted any reference to "Capital One" or "Cap One."[4] (*Id*.)

---

[3] Mr. Kennedy also avers that "Capital One had requested that TrustedSec destroy documents, and TrustedSec complied with that request consistent with its contractual obligations with Capital One; however, TrustedSec was able to recover and produce all of those documents to the plaintiffs." (*Id*. at ¶ 9.)

[4] For example, the revised search terms included the following: (1) ("Security Information and Event Management" OR SIEM); (2) "Cloud Custodian"; (3) (GuardDuty OR "Guard Duty"); (4) ((IAM OR "identity and access management" OR "identity management") w/100 permission*); (5) ("instance metadata service" OR "IMS"); (6) (Cyber* AND (budget OR spend*)); and (7) (Encrypt* w/10 (data OR "PII" OR "personally-identifiable information" OR "personally identifiable information" OR (customer w/5 (information OR data) OR s3 OR bucket*)). (Doc. No. 9-2 at PageID# 262.)

TrustedSec objected, asserting that "your revised search terms only broadened the earlier ones, by removing any relationship whatsoever to Capital One (excepting [terms] 29 -31), thereby rendering them wildly overbroad." (Doc. No. 1-3 at PgaeID# 107.) TrustedSec advised Plaintiffs that it had believed it had substantially complied with its obligations under the non-party subpoena. (*Id.*)

On October 16, 2020, Plaintiffs sent an email to TrustedSec demanding that it (1) "cooperate in drafting mutually agreed search terms that return a reasonable volume of responsive documents;" (2) provide project names, internal terminology used by TrustedSec on Capital One cybersecurity projects, and identify how TrustedSec documents refer to Capital One; (3) "cooperate in using hit reports to revise search terms through an iterative process to arrive at mutually agreed search terms that target responsive documents;" (4) "cooperate in some testing and quality control of the documents identified by the search terms;" (5) produce documents for the period January 1, 2018 to June 1, 2020; (6) substantially complete its production within 14 days of final agreed search terms; and (7) make its production in compliance with the ESI protocol entered in the underlying MDL litigation. (Doc. No. 1-3 at PageID# 110.) TrustedSec declined, asserting that it had already produced all the documents in its possession relating to its work for Capital One.

On October 28, 2020, Plaintiffs filed a Motion in this Court to Transfer to the MDL Court or, in the Alternative, to Compel TrustedSec to comply with the subpoena.[5] (Doc. No. 1.) TrustedSec

[5] Portions of the Memorandum in Support of Plaintiffs' Motion are redacted. In addition, several exhibits attached to Plaintiffs' Motion (i.e., Exhibits 4, 5, 7, 8, and 10 to the Declaration of Steve Six) are not included on the public docket but simply marked as "sealed." (Doc. No. 1-3 at PageID# 69, 70, 75, 76, 79.) Thus, in conjunction with its Motion to Transfer or Compel, Plaintiffs filed a Motion to File Documents under Seal. (Doc. No. 2.) On October 29, 2020, this Court denied Plaintiffs' Motion to Seal on the grounds that Plaintiffs had failed to "analyze, in detail, document by document, the propriety of secrecy" with respect to the information they sought to submit under seal. (Doc. No. 5.) The Court ordered Plaintiffs to either (1) file a non-redacted version of their Memorandum in Support of Motion to Transfer with full and complete copies of Exhibits 4, 5, 7, 8, and 10; or (2) file a supplemental brief that provides a more complete and thorough justification for their request to file under seal. (*Id.*) On November 2, 2020, Plaintiffs filed a Supplemental Brief in support of their Motion to Seal. (Doc. No. 6.) Shortly thereafter, on November 6, 2020, the Court issued an

filed its Brief in Opposition to Plaintiffs' Motion to Transfer or, in the Alternative, to Compel on November 11, 2020. (Doc. No. 9.) Plaintiffs filed a reply in support of their Motion on November 18, 2020. (Doc. No. 10.) On November 19, 2020, TrustedSec was granted leave to file a sur-reply instanter. (Doc. No. 12.) Thus, this matter is now ripe and ready for resolution.

II. Analysis

In their Motion, Plaintiffs argue that transfer to the MDL court is warranted because that court "is familiar with the complex issues, has a strong interest in managing its schedule, and can better-avoid inconsistent rulings in other districts where subpoenas are pending." (Doc. No. 1-1 at p. 3.) In the alternative, Plaintiffs assert that TrustedSec should be ordered to comply with the subpoena because the requested information is relevant and the subpoena is not unduly burdensome. (*Id*. at 9-15.) Plaintiffs ask this Court to order TrustedSec to (1) cooperate in drafting mutually agreed search terms; (2) provide project names, and internal terminology used by TrustedSec for Capital One cybersecurity projects and identify how TrustedSec documents refer to Capital One; (3) cooperate in using hit reports to revise search terms through an iterative process to arrive at mutually agreed search terms that target responsive documents; (4) cooperate in testing and quality control of the documents identified by the search terms; (5) use best efforts to complete this process on search terms, project names, and quality control testing within 7 days of this Court granting the Motion to Compel; (6) produce documents for the period January 1, 2018 to June 1, 2020; and (7) substantially complete its production within 21 days of this Court granting a Motion to Compel. (*Id*. at p. 15.)

Order granting in part and denying in part Plaintiffs' request to file certain documents and information under seal. (Doc. No. 7.) Plaintiffs were directed to file the requested documents and information under seal, which they did on November 9, 2020. (Doc. No. 8.)

TrustedSec argues that transfer is inappropriate because it has substantially complied with the subpoena, and "the issues here are narrow and unique to this dispute [and] there is no threat of inconsistent rulings that might otherwise warrant transfer." (Doc. No. 9 at p. 2.) TrustedSec further maintains that Plaintiffs' Motion to Compel should be denied because it has produced "all of the documents it believes it has related to its work for Capital One" and "there is nothing further to compel." (*Id.* at p. 7-9.) In addition, TrustedSec maintains that Plaintiffs' proposed "iterative" process of running multiple searches and hit reports with revised search terms is disproportional to the needs of the case and would impose an undue burden. (*Id*. at p. 9-10.) Lastly, TrustedSec argues that Plaintiffs have abused their subpoena power and should be required to pay for TrustedSec's expenses, including attorney fees, for having to "respond to Plaintiffs' demands and defend against Plaintiffs' motion to transfer or compel and related filings." (*Id*. at pp. 14-15.)

In reply, Plaintiffs argue that it is TrustedSec that has behaved unreasonably in refusing to engage in a cooperative process to develop and refine search terms through the use of hit reports. (Doc. No. 10 at p. 12.) Plaintiffs argue that "every other entity in the MDL" has agreed to the search methodology proposed herein and TrustedSec's opposition is "frivolous." (*Id*.) Plaintiffs argue that they (as opposed to TrustedSec) should be awarded attorney's fees "for being put to the task of bringing this Motion." (*Id.*)

The Court will first address Plaintiffs' request for transfer under Fed. R. Civ. P. 45(f).

A. Motion to Transfer

Federal Rule of Civil Procedure 45(f)[6] provides as follows:

---

[6] Federal Rule of Civil Procedure 45 provides a mechanism for parties to an action to obtain discovery, including production of documents and deposition testimony, from a nonparty. *See Kennedy v. Caruso*, 2020 WL 2815137 at * 1 (M.D. Tenn. May 5, 2020). A subpoena under Rule 45 "must issue from the court where the action is pending." Fed. R.

> **(f) Transferring a Subpoena-Related Motion.** When the court where compliance is required did not issue the subpoena, it may transfer a motion under this rule to the issuing court if the person subject to the subpoena consents or if the court finds exceptional circumstances. Then, if the attorney for a person subject to a subpoena is authorized to practice in the court where the motion was made, the attorney may file papers and appear on the motion as an officer of the issuing court. To enforce its order, the issuing court may transfer the order to the court where the motion was made.

In evaluating whether there are "exceptional circumstances" warranting transfer, "[t]he prime concern should be avoiding burdens on local nonparties subject to subpoenas, and it should not be assumed that the issuing court is in a superior position to resolve subpoena-related motions." Advisory Committee Notes, Fed. R. Civ. P. 45 (2013 Amendments). However, in some circumstances, transfer may be warranted "in order to avoid disrupting the issuing court's management of the underlying litigation, as when that court has already ruled on issues presented by the motion or the same issues are likely to arise in discovery in many districts." *Id.* Transfer is appropriate only if such interests outweigh the interests of the nonparty served with the subpoena in obtaining local resolution of the motion. *Id. See also Parker Compound Bows, Inc. v. Hunter's Manufacturing Co., Inc*., 2015 WL 7308655 at * 1 (N.D. Ohio Nov. 19, 2015).

The proponent of transfer bears the burden of showing that extraordinary circumstances are present. *See* Advisory Committee Notes, Fed. R. Civ. P. 45 (2013 Amendments). In determining whether transfer is appropriate under Rule 45(f), federal courts have considered a number of factors, including "'case complexity, procedural posture, duration of pendency, and the nature of the issues pending before, or already resolved by, the issuing court in the underlying litigation.'" *Parker*

Civ. P. 45(a)(2). A person seeking to enforce or challenge a subpoena must do so in "the court for the district where compliance is required." Fed. R. Civ. P. 45(d)(3)(A). Here, the instant subpoena to TrustedSec was issued by the MDL court; i.e., the United States District Court for the Eastern District of Virginia. TrustedSec, however, is located in this District. Because compliance is required in this District, Plaintiffs filed the instant action in this Court.

Compound Bows, Inc., 2015 WL 7308655 at * 1 (quoting *Judicial Watch, Inc. v. Valle Del Sol, Inc.*, 307 F.R.D. 30, 34 (D.D.C. 2014)). *See also e.g., Fed. Home Loan Mortgage Corp. v. Deloitte & Touche LLP*, 309 F.R.D. 41, 44 (D.D.C.2015). The decision of whether to transfer is discretionary. *See, e.g., Federal Trade Commission v. A+ Financial Center, LLC*, 2013 WL 6388539 at * 2-3 (S.D. Ohio Dec. 6, 2013); *Moon Mountain Farms LLC v. Rural Community Insurance Co.*, 301 F.R.D. 426, 429 (N.D. Cal. 2014).

Plaintiffs argue that exceptional circumstances warrant transfer of the instant dispute to the MDL court. They maintain that the "MDL court is better positioned to assess this dispute" because the Capital One data breach case is both procedurally and substantively complex and has been pending for more than a year. (Doc. No. 1-1 at p. 5.) Plaintiffs note that "the MDL court has already made three rulings involving privilege and work product disputes related to" two other cybersecurity third-party subpoena recipients and, therefore, that court "developed an understanding of the factual predicates implicated in the subpoena dispute." (*Id.* at p. 6.) Plaintiffs further assert that transfer would prevent the likelihood of inconsistent rulings "on intertwined Capital One and third-party discovery issues." (*Id.*) Plaintiffs state that they have served 11 subpoenas on third-party entities that provided cybersecurity services for Capital One and that "the risk of inconsistent rulings" is high absent transfer. (*Id.* at p. 7.) Finally, Plaintiffs maintain that "there is no burden imposed on TrustedSec in transfer to the issuing MDL court" because proceedings in that court are currently being held remotely due to COVID-19. (*Id.* at p. 8.)

TrustedSec argues that transfer is not appropriate because the instant dispute "is only about whether [it] already substantially complied with Plaintiffs' subpoena" and is, therefore, a narrow dispute that does not relate to any substantive matters at issue in the MDL litigation. (Doc. No. 9 at

p. 11.) Relatedly, TrustedSec asserts that there are no "intertwined issues" with either Capital One or any other non-parties to the MDL litigation. (*Id*.) TrustedSec also argues that it is immaterial that the MDL court has taken up subpoena-related discovery motions regarding privilege and work product issues since TrustedSec is not withholding any documents on that basis. (*Id.* at p. 11-12.) Finally, TrustedSec argues that it would suffer an undue burden if this dispute were transferred because it "would be required to retain local counsel, and local counsel would have to analyze the facts and law to properly defend TrustedSec against Plaintiffs' motion, all at additional and duplicative expense to TrustedSec." (*Id.* at p. 12.)

For the following reasons, the Court finds that Plaintiffs have failed to demonstrate extraordinary circumstances warranting transfer to the MDL court. First, the Court agrees with TrustedSec that the instant dispute is not intertwined with, or otherwise related to, any procedural or substantive issues being litigated in the MDL litigation. The primary issue here is whether TrustedSec substantially complied with the subpoena when it failed to engage in the "iterative process" proposed by Plaintiffs with regard to the production of TrustedSec's ESI. Plaintiffs have failed to demonstrate that this narrow, fact-specific issue relates to any of the complex procedural or substantive issues in the underlying MDL litigation, nor have Plaintiffs demonstrated that the MDL court is in a superior position to resolve the instant dispute. Moreover, although the MDL court has apparently ruled on several privilege and work product disputes relating to third party entities, no such issues are presented by the instant Motion. Indeed, TrustedSec expressly states that it is not withholding any responsive documents on the basis of either attorney-client privilege or work product. (Swing Decl. (Doc. No. 9-2) at ¶ 11.)

The Court further finds that Plaintiffs have failed to demonstrate a risk of inconsistent rulings. Plaintiffs argue this risk is high because they intend to raise a spoliation issue regarding Capital One with the MDL court regarding the fact that Capital One instructed TrustedSec to destroy certain documents after the March 2019 breach. (Doc. No. 1-1 at p. 7.) TrustedSec's CEO David Kennedy, however, expressly avers that TrustedSec recovered and produced all such documents to Plaintiffs in response to the instant subpoena.[7] (Kennedy Decl. (Doc. No. 9-1) at ¶ 9.) Moreover, although Plaintiffs issued similar subpoenas to other third-party cybersecurity entities, it has not demonstrated that the Court's resolution of the very specific discovery issue currently before it poses any risk of inconsistent rulings warranting transfer.

Finally, the Court agrees with TrustedSec that transfer would impose an undue burden. As noted above, the Advisory Committee Notes to Rule 45 caution that "[t]he prime concern should be avoiding burdens on local nonparties subject to subpoenas." Advisory Committee Notes, Fed. R. Civ. P. 45 (2013 Amendments). Here, should the Court transfer this dispute, TrustedSec will be required to defend against Plaintiffs' Motion in the Eastern District of Virginia. TrustedSec avers (and Plaintiffs do not contest) that this would require it to find and hire local counsel and pay attorney's fees associated with getting local counsel up to speed on the instant dispute. Under the circumstances presented, the Court finds that the balance of interests does not "outweigh the interests of the nonparty served with the subpoena in obtaining local resolution of the motion." *Id. See also Parker Compound Bows, Inc.*, 2015 WL 7308655 at * 1.

---

[7] Specifically, Mr. Kennedy avers that: "Capital One had requested that TrustedSec destroy documents, and TrustedSec complied with that request consistent with its contractual obligations with Capital One; however, TrustedSec was able to recover and produce all of those documents to the plaintiffs." (Kennedy Decl. (Doc. No. 9-1) at ¶ 9.)

Accordingly, and for all the reasons set forth above, the Court finds that Plaintiffs have failed to demonstrate extraordinary circumstances warranting a transfer to the MDL court. Plaintiffs' request to transfer is, therefore, denied.

B. Motion to Compel

Alternatively, Plaintiffs argue that the Court should compel TrustedSec to comply with the subpoena. (Doc. No. 1-1 at pp. 9-15.) Plaintiffs assert that the requested information is relevant and is not limited to testing of the particular vulnerability the hacker used to access Capital One's consumer information in the 2019 breach. (*Id*. at p. 9.) Rather, Plaintiffs assert that the subpoena also seeks relevant information regarding the "budget TrustedSec requested versus what Capital One provided; the amount of time TrustedSec needed for the testing versus what Capital One permitted; and the types of testing services TrustedSec suggested versus what Capital One provided." (*Id*. at p. 12.)

Plaintiffs further argue that requiring TrustedSect to engage in an "iterative" process to develop and refine ESI search terms to capture this information does not impose an undue burden. (*Id*. at p. 13.) Citing Appendix K of this District's Local Rules,[8] Plaintiffs assert that "[t]he use of agreed search terms is an approach to electronic discovery used in this district." (*Id*.) Plaintiffs argue that, although they proposed the initial search terms, "that does not change the fact that the terms were not agreed, not final, and not tested to see if they returned responsive documents before

[8] Appendix K is entitled "Default Standard for Discovery of Electronically Stored Information." It provides, in relevant part, that "[t]he court expects the parties to cooperatively reach agreement on how to conduct e-discovery." App. K, Para. 1. Appendix K further states that: "If the parties intend to employ an electronic search to locate relevant electronically stored information, the parties shall disclose any restrictions as to scope and method which might affect their ability to conduct a complete electronic search of the electronically stored information. The parties shall reach agreement as to the method of searching, and the words, terms, and phrases to be searched with the assistance of the respective e-discovery coordinators, who are charged with familiarity with the parties' respective systems." App. K. Para. 6.

TrustedSec used them for collection and production." (*Id.* at p. 14.) Plaintiffs assert that running additional searches based on revised search terms would not impose an undue burden on TrustedSec and that it should be required to cooperate in drafting mutually agreed search terms, provide project names and internal terminology, cooperate in using hit reports to revise search terms, and engage in testing and quality control of the documents identified by search terms. (*Id*.)

TrustedSec insists that it "has produced to Plaintiffs what it believes are all of the documents in its possession related to its work for Capital One" and "there is nothing further to compel." (Doc. No. 9 at pp. 1, 7.) It notes that "Plaintiffs have not identified any specific documents or information that they are looking for from TrustedSec or have reason to believe exist related to Capital One as a basis for further discovery." (*Id*. at p. 7.) TrustedSec emphasizes that it engaged in good faith negotiations with Plaintiffs' counsel for over four months and has produced over 9,000 pages of documents in response to the subpoena at issue. (*Id*. at pp. 1-2.) TrustedSec argues that "such diligent cooperation does not merit forcing a subpoena recipient to engage in an indefinite 'iterative process' in search of more documents for which there is no reason to believe they exist." (*Id*. at p. 8.)

In reply, Plaintiffs argue that "TrustedSec's belief about what ESI exists is cabined to the ESI collected with the deficient search terms." (Doc. No. 10 at p. 4.) They assert that TrustedSec "has conducted no investigation into what ESI exist beyond what it collected from the deficient search terms and makes no such claims of investigation in its supporting declarations." (*Id*.) Plaintiffs repeatedly complain about TrustedSec's failure to engage in a cooperative process of using "hit reports" to refine the ESI search terms, arguing that "TrustedSec's search methodology combined the worst of both worlds by using untested, draft terms that resulted in the production of useless documents, and at the same time provides no confidence that relevant, responsive, and proportional

documents have been produced." (*Id*. at p. 7.) Plaintiffs assert that this Court should order TrustedSec to comply with the subpoena because "the only substantial burden is of TrustedSec's own making." (*Id.* at p. 8.)

The scope of a subpoena issued under Fed. R. Civ. P. 45 is "subject to the general relevancy standard applicable to discovery under Fed. R. Civ. P. 26(b)(1)." *Laetham Equip. Co. v. Deere and Co*., 2007 WL 2873981 at * 4 (E.D. Mich. Sept. 24, 2007). Although irrelevance or overbreadth are not specifically listed under Rule 45 as a basis for quashing a subpoena, courts "have held that the scope of discovery under a subpoena is the same as the scope of discovery under Rule 26." *Hendricks v. Total Quality Logistics*, 275 F.R.D. 251, 253 (S.D. Ohio 2011). In addition, a court must quash any subpoena that imposes an undue burden or expense on the person subject to the subpoena, fails to allow reasonable time to comply, requires compliance beyond the geographic limits of Rule 45, or requires disclosure of "privileged or other protected matter, if no exception or waiver applies." Fed. R. Civ. P. 45(d)(1), (d)(3)(A)(i)-(iv). *See B.L. Schuhmann*, 2020 WL 3145692 at * 2 (W.D. Ky. June 12, 2020).

Whether a subpoena imposes an undue burden should be assessed "in a case-specific manner considering 'such factors as relevance, the need of the party for the documents, the breadth of the document request, the time period covered by it, the particularity with which the documents are described and the burden imposed.'" *In re: Modern Plastics Corp.*, 890 F.3d 244, 251 (6th Cir. 2018) (quoting *Am. Elec. Power Co., Inc. v. United States*, 191 F.R.D. 132, 136 (S.D. Ohio 1999)). *See also Baumer v. Schmidt*, 423 F.Supp.3d 393, 398 (E.D. Mich. 2019) ("To determine whether a burden is undue, a court must balance the potential value of the information to the party seeking it against the cost, effort, and expense to be incurred by the person or party producing it." (quoting *EEOC v.*

Ford Motor Credit Co., 26 F.3d 44, 47 (6th Cir. 1994)); *Arriola v. Commonwealth of Kentucky*, 2020 WL 6568848 at * 1 (E.D. Ky. Nov. 9, 2020). In making this assessment, "[c]ourts must 'balance the need for discovery against the burden imposed on the person ordered to produce documents,' and the status of that person as a non-party is a factor." *In re: Modern Plastics Corp*., 890 F.3d at 251.

For the following reasons, Plaintiffs' Motion to Compel is denied. As detailed in Section I of this Opinion, TrustedSec worked with Plaintiffs' counsel in good faith for over four months to comply with the subpoena at issue. Plaintiffs do not dispute that, in response to the subpoena, TrustedSec promptly produced its master services agreement with Capital One and all of the technical consulting reports for its work, along with written information relating to (1) the dates that TrustedSec provided network security services to Capital One, including the dates of specific testing; (2) the names of the TrustedSec employees that interacted with Capital One regarding penetration testing services; and (3) the names of the Capital One employees that TrustedSec interacted with regarding penetration testing. (Doc. No. 8-6 at PageID#s 219-229) (filed under seal). In addition, TrustedSec searched its internal email, external email, and instant messaging service using the 34 search terms/phrases that Plaintiffs themselves proposed on August 5, 2020. Many of these initial search terms were quite broad in scope and required TrustedSec to search for all ESI that mentioned Capital One and such topics as "identity management," cyber budgets and spending, data encryption, vulnerabilities in cardholder data environments, exfiltration risks, cyber maturity, and data loss prevention. (Doc. No. 9-2 at PageID#s 259-260.)

TrustedSec performed the search criteria "over the entire Exchange infrastructure," requiring it "to create custom queries through the SQL database through the chat software (MatterMost) which required extensive work in order to decrypt the SQL table structures with the encryption keys and

extract the appropriate search terms through the database itself." (Kennedy Decl. (Doc. No. 9-1) at ¶ 6.) After conducting this search, TrustedSec supplemented its production with over 1,500 emails and messages. (Swing Decl. (Doc. No. 9-2) at ¶ 10.) Mr. Kennedy submitted a Declaration regarding the substantial time, effort, and expense involved in responding to the subpoena, estimating that it took TrustedSec personnel 63 hours to gather this information at an internal cost of $18,900. (Kennedy Decl. (Doc. No. 9-1) at ¶ 8.) Mr. Kennedy further avers that "TrustedSec has provided all related search terms, results, documents, and data related to Capital One." (*Id*. at ¶ 6.)

Plaintiffs now complain that the search terms that they themselves proposed are "deficient" and that the documents produced by TrustedSec as a result of that search are "useless." (Doc. No. 10.) As TrustedSec correctly notes, however, Plaintiffs have not identified any specific documents or information (or categories of documents or information) that they believe may exist but were not produced.[9] Rather, Plaintiffs simply appear to be dissatisfied with the results of TrustedSec's search and now seek to broaden the search terms to include documents relating to a host of topics regardless of whether those documents have any specific connection to Capital One. Indeed, in their October 12, 2020 revised search terms, Plaintiffs delete all references to Capital One and demand that TrustedSec run searches for such general topics as "security information and event management," "identity and access management," cyber budgets and spending, exfiltration risks, cyber w/20 maturity, log w/20 retention, cardholder data vulnerabilities, and data loss prevention. (Doc. No. 9-

[9] Plaintiffs complain that they are entitled to information regarding "the budget TrustedSec requested versus what Capital One provided; the amount of time TrustedSec needed for the testing versus what Capital One permitted; and the types of testing services TrustedSec suggested versus what Capital One provided." (Doc. No. 1-1.) However, Plaintiffs do not explain why they believe this information would not have been captured through TrustedSec's searches using Plaintiffs' initial 34 search terms. Indeed, several of these terms would appear to expressly include such information, such as the search term "cyber* AND (budget OR spend*)) AND ("Capital One" OR "CapitalOne" OR "Cap One" OR "CapOne" or @capitalone.com).

2 at PageID#s 261-262.) The Court agrees with TrustedSec that Plaintiffs' revised search terms are extremely overbroad and not proportional to the needs of the case.

The Court also rejects Plaintiffs' argument that Appendix K to this Court's Local Rules requires TrustedSec to engage in the "iterative" process it proposes. Appendix K sets forth a default standard for conducting e-discovery for *parties* to lawsuits in this District. TrustedSec, however, is not a party to the underlying MDL litigation. It is a non-party recipient of a Rule 45 subpoena. Plaintiffs cite no binding authority that TrustedSec is bound by Appendix K under the circumstances presented. Nor have Plaintiffs cited any binding authority that TrustedSec (as a non-party subpoena recipient) should be required to engage in Plaintiffs' proposed ESI search process where it has already incurred significant time and expense in searching its ESI using a broad set of multiple search terms proposed by Plaintiffs themselves. This is particularly the case where Plaintiffs have failed to adequately demonstrate either that the documents already produced are insufficient or that additional searches would be likely to uncover previously undisclosed responsive information. Under the circumstances presented, the Court finds that Plaintiffs' request that TrustedSec be ordered to engage in an indefinite "cooperative" process of developing, refining, and running multiple additional searches is not reasonable and would impose an undue burden on TrustedSec.

Accordingly, and for all the reasons set forth above, Plaintiffs' Motion to Compel is denied. With regard to TrustedSec's request for attorney fees in responding to Plaintiffs' Motion, this request is denied. While the Court ultimately disagrees with Plaintiffs' position, TrustedSec has not demonstrated that Plaintiffs' Motion was frivolous or otherwise so meritless as to warrant an award of attorney fees.

III. Conclusion

Accordingly, and for all the foregoing reasons, Plaintiffs' Motion for Transfer, or in the Alternative, to Compel (Doc. No. 1) is DENIED. TrustedSec's request for attorney fees is DENIED. This action is hereby terminated.

IT IS SO ORDERED.

s/Pamela A. Barker
PAMELA A. BARKER
U. S. DISTRICT JUDGE

Date: November 20, 2020