UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

DIGITAL ASSURANCE CERTIFICATION, LLC,

Plaintiff,

v. Case No: 6:17-cv-72-Orl-41TBS

ALEX PENDOLINO, JR.,

Defendant.

ORDER

This case comes before the Court without oral argument[1] on the following motions and responses:

- Non-Party Lumesis, Inc. Motion to Quash Plaintiff Digital Assurance Certification, LLC's Subpoena in a Civil Action (Doc. 67);
- Plaintiff's Amended Motion to Compel Discovery Responses from Lumesis, Inc. (Doc. 68);
- Non-Party Lumesis, Inc.'s Response to Plaintiff's Amended Motion to Compel (Doc. 72); and
- Plaintiff's Response to Lumesis, Inc.'s Motion to Quash (Doc. 73).

Because the motions to quash and to compel concern the same subpoena, the Court deals with them at the same time in this Order.

Background

Plaintiff Digital Assurance Certification, LLC ("DAC") helps the issuers of municipal bonds and private sector borrowers of municipal bond proceeds comply with Securities

---

[1] Plaintiff requested oral argument on its motion to compel (Docs. 66, 69). Those requests are **DENIED**.

and Exchange Commission regulations and post-issuance tax requirements (Doc. 1 at ¶ 6). It also acts as a dissemination agent for required and voluntary disclosures made by bond issuers (Id.). DAC alleges that a critical component of its business is a summary page it developed (Id. at ¶ 8). The summary page includes representations and tools to assist issuers in complying with their obligations owed to the investment community (Id.). The summary page also provides a means for issuers to post information concerning their bonds so that it is available to the investment community (Id.). DAC has expended considerable sums of money to develop, maintain and upgrade the summary page (Id. at ¶ 9). To protect the summary page and its other confidential and proprietary information, DAC enters into confidentiality agreements with its employees and clients (Id. at ¶¶ 13, 16).

On August 6, 2013, DAC employed Defendant Alex Pendolino, Jr. as a broker-dealer liaison (Id. at ¶ 3). In that capacity, he "was responsible for communicating with client compliance officers and bankers regarding specific bond offerings of issuers to be reviewed, the parameter of such reviews, any relevant factual context and other related matters." (Doc. 60-1 at ¶ 56). Pendolino also performed broker-dealer compliance reviews (Id.). At the start of his employment, Pendolino signed a confidentiality agreement in which he acknowledged that he would be receiving DAC's confidential, proprietary information which he promised not to disclose to unauthorized persons (Id. at ¶ 14). On October 10, 2016, Pendolino delivered his resignation letter to DAC (Id. at ¶ 21). The next day, DAC informed Pendolino that it had not accepted his resignation and that he was being terminated for cause effective October 10, 2016 (Id. at ¶ 23).

DAC alleges that while employed, Pendolino was in possession of client contracts containing proprietary secrets including the identity of DAC's clients, pricing information

and information about customized services provided to those clients (Doc. 60-1 at ¶ 63). This information, which was usually kept in Pendolino's office, could not be located after he ceased working for the company (Id.).

In November 2016, Pendolino went to work as a data analyst for DAC's competitor, Lumesis, Inc. (Doc. 1 at ¶ 26). In his current job, Pendolino analyzes underwriting deals identified by Lumesis' clients, using Lumesis' proprietary DIVER Underwriter Platform (Doc. 67 at 2). According to Lumesis, Pendolino's current job is different than the work he did as a broker-dealer for DAC (Id. at 2, n. 2).

After Pendolino left its employ, DAC engaged a computer forensics expert to examine his former work computer (Doc. 1 at ¶ 29). The expert has opined that on October 5 and 10, 2016, Pendolino attached a USB drive to his work laptop and accessed every document on DAC's shared drive (Id. at ¶ 30). The expert is unable to say whether Pendolino copied any of DAC's documents to the USB drive (Id.). DAC alleges that Pendolino had no business reason to access this information (Id.). In the forensic computer examiner's opinion:

> Based on analysis of the laptop alone, it is not possible to determine if data was copied to the USB device, and, if data was copied, specifically what data, but I observed no evidence indicating any other reason for attaching the USB device to the laptop. While the USB device was attached to the computer multiple times, there is no evidence of it being used for other purposes. The best method to determine if data was copied to the USB device would be to forensically examine the USB device itself.

(Doc. 5 at 7).

DAC alleges that after Pendolino joined Lumesis, one of its clients moved its business to Lumesis (Id. at ¶ 27). The client told DAC that Lumesis was developing its own summary page, which was substantially similar to DAC's summary page (Id.).

Lumesis claims that the client began doing business with it months before it hired Pendolino (Doc. 67-6 at 3). After Pendolino joined Lumesis, DAC learned that Lumesis had solicited another one of its clients, and was offering to provide services similar to those provided by DAC at a lower price (Doc. 75, ¶ 68).

DAC alleges that Pendolino stole its confidential client files and trade secret information including the identity of clients, pricing information, the services and processes it provides to each client, and analyses by DAC of its clients' regulatory obligations and compliance history (Id. at ¶¶ 24-25, 31). DAC's complaint against Pendolino contains counts for: (1) violation of the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836; (2) violation of the Florida Uniform Trade Secrets Act, FLA. STAT. § 688.01 *et seq.*; (3) breach of the confidentiality agreement; and (4) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Id.). Pendolino denies taking DAC's confidential, proprietary information (Doc. 43 at 10). He also denies providing any of DAC's confidential information to Lumesis (Id. at 15).

In January 2017, DAC sent a litigation hold letter to Lumesis (Doc. 67 at 3). Lumesis represents that it complied with the letter and that it conducted its own internal investigation to determine whether it had received confidential information from Pendolino (Id.). The Lumesis investigation included an examination of Pendolino's work computer including the hard drive, recycle bin, email, and all interfaces with Lumesis' network systems, cloud network and storage systems (Id. at 3-4). Lumesis also sought to determine whether Pendolino had inserted the USB drive into his work computer and has concluded that he did not (Id. at 4). It also interviewed its employees and management who work with Pendolino (Id.). As result of this investigation, Lumesis asserts that it has not received any disclosure from Pendolino that would violate his confidentiality

agreement with DAC (Id.). On February 2, 2017, Lumesis sent DAC a letter, informing it of the results of this investigation (Id. at 4).

Pendolino filed a motion to dismiss DAC's complaint and DAC filed a motion to amend its complaint (Docs. 45, 60). On September 27, 2017 the Court granted DAC leave to file an amended complaint and denied the motion to dismiss as moot (Doc. 74). However, the Court did find that DAC's claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) was not properly brought and should be omitted from the amended complaint (Id.). DAC filed its amended complaint on September 28. The amended complaint adds Lumesis as a Defendant (Doc. 75). In the amended complaint, DAC accuses Lumesis of misappropriation of its trade secrets and tortious interference in its business relationship with Pendolino (Id. at ¶¶ 79-80, 96-100).

In discovery propounded to Pendolino, DAC sought information concerning Lumesis (Doc. 73 at 6). Pendolino responded that his Lumesis work computer and the information stored on it, together with materials provided to him and contained on the Lumesis's network belong to Lumesis and therefore, he cannot produce them (Id.). Among other things, DAC asked Pendolino to produce:

> Any program or service used to store any of DAC's Confidential or Trade Secret Information or any Documents that contain DAC's Confidential or Trade Secret Information.

(Id.). Pendolino's objection to this request ended with the following statement:

> Finally, Defendant objects to the production of any electronic device, program or service to the extent that it is owned by Lumesis, Inc. and not by Defendant.

(Id.). DAC believes this response is an indication that its "confidential or trade secret information has been placed on or is stored on Lumesis's system." (Id.). DAC asserts that "[b]ecause Pendolino's responses indicate that DAC documents may reside on his

Lumesis-issued computer, or in Lumesis's network system, and further state that he is not authorized to produce such documents, DAC was left with no choice other than to seek the documents from Lumesis." (Id. at 7). On May 9, 2017, DAC served a subpoena for the following information on Lumesis:

> 1. The Windows System and User Registries[2] (or functional equivalent for non-Windows devices) for any computer device (including laptops, desk computers, and tablets) issued to Pendolino by Lumesis, including the Dell XPS desk top computer, serial number H080KB2, and including information sufficient to show all data related to installed software, and external hardware devices connected to each such computer device.
>
> 2. The Master File Table[3] (or functional equivalent for non-windows devices) (including Filename, File Path,[4] Last Modified, Last Accessed, Created and Entry Modified date and time stamps) for any computer device (including laptops, desk computers, and tablets) issued to Pendolino by Lumesis, including the Dell XPS desk top computer, serial number H080KB2, and including information sufficient to identify the complete file structure and distinct folders.

---

[2] Per the Court's research, "User registries store user account information, such as user ID and password, that can be accessed during authentication. User repositories store user profiles and preference information. A user registry or repository is used to: Authenticate a user using basic authentication, identity assertion, or client certificates." https://www.ibm.com/support/knowledgecenter/en/SSYJ99_8.0.0/.../plan_ureg.html.

[3] A "Master File Table" is: "The primary record of file storage locations on a Microsoft Windows based computer employing NTFS filing systems." The Sedona Conference Glossary: E-Discovery and Digital Information Management (Fourth Edition). NFTS or New Technology File System is "A high-performance and self-healing file system proprietary to Microsoft, used in Windows NT, Windows 2000, Windows XP and Windows Vista Operating Systems, that supports file-level security, compression and auditing. It also supports large volumes and powerful storage solutions such as Redundant Array of Inexpensive Disks (RAID). An important feature of NTFS is the ability to encrypt files and folders to protect sensitive data." Id.

A "Master File Table" is also defined as "a database in which information about every file and directory on an NT File System (NFTS) volume is stored. There is at least one record for every file directory on the NFTS logical volume. Each record contains attributes that tell the operating system (OS) how to deal with the file or director associated with the record." Searchwindowsserver.techtarget.com/definition/master-file-table.

[4] A "file" is: "A collection of related data or information stored as a unit under a specified name on storage medium." Sedona. A "file path describes the location of a file in a web site's folder structure." https://www.w3schools.com/html/html_filepaths.asp.

3. The Internet History and temporary file cache[5] files for any computer device (including laptops, desk computers, and tablets) issued to Pendolino by Lumesis, including the Dell XPS desk top computer, serial number H080KB2, and including information disclosing the Internet History activity of the custodian of such computer device.

4. A file listing of all Cloud Storage (including Drop box, OneDrive, Google Drive) files synchronized locally for any computer device (including laptops, desk computers, and tablets) issued to Pendolino by Lumesis, including the Dell XPS desk top computer, serial number H080KB2, and including information disclosing the Internet History of the custodian of such computer device.

5. All link files (.LNK)[6] and Jump List[7] entries from each custodian of any computer device (including laptops, desk computers, and tablets) issued to Pendolino by Lumesis, including the Dell XPS desk top computer, serial number H080KB2, sufficient to show the usage of relevant files, regardless of where those files were stored.

---

[5] A "cache" is: "A dedicated, temporary, high speed storage location that can be used to store frequently-used data for quick user access, allowing applications to run more quickly." Sedona. A "temporary file cache" is a reference to the following: "Each time a user visits a website using Microsoft Internet Explorer, files downloaded with each web page (including HTML and Javascript code) are saved to the Temporary Internet Files folder, creating a web cache of the web page on the local computer's hard disk drive, or other form of digital data storage. The next time the user visits the cached website, only changed content needs to be downloaded from the Internet; the unchanged data is available in the cache. Despite the name 'temporary', the cache of a website remains stored on the hard disk until the user manually clears the cache, the cache expires or if the cache is full. This is often regarded as a privacy issue, because anyone with access to the computer can view the cache. The contents of the folder are indexed using an index.dat file, a form of database. The Temporary Internet Files cache can be useful in certain situations. For example, if no Internet connection is available, previously cached websites are still available offline. Certain online media files (such as embedded Flash movies) are not easily accessed directly through Internet Explorer, but are automatically saved into the cache after viewing them. Depending on the type of website and how often it is updated, the cached data may not reflect the online version of the website. The cache is also useful for police to collect forensic evidence." https://en.wikipeia.org/wiki/Temporary_Internet-Files.

[6] DAC's expert explains that "link files" are "shortcuts created automatically by the Windows OS when a file is accessed to facilitate the user locating the file the next time it is desired." (Doc. 5, n. 4). According to the Court's research, a "link file" "is the nickname for any file that contains a reference to another file or directory in the form of an absolute or relative path and affects pathname resolution." https://en.wikipedia.org/wiki/Symbolic-Link. Apparently, "[e]ach link file has its own Created, Modified and Accessed dates and within each link file there are Created, Modified and Accessed dates which belong to the target file. In addition, if the target file still exists on the media, that file has its own three dates." Computerforensics.parsonage.co.uk/downloads/themeaningoflife.pdf.

[7] A "Jump List is a feature introduced in Windows 7. This feature allows you to view recent documents in a program that is pinned to your taskbar. To do this, right-click on any program that has an icon in the taskbar, and it will bring up a list of recently modified documents within that program." https://www.computerhope.com/jargon/j/jumplist.htm.

6. Each DAC Document or information that resided on, or was transferred to, or was stored for any period of time on or in any computer hard drive, recycle bin, email system, database, shared network drive, cloud network interface, storage provider, electronic interface or other storage medium to which Pendolino or Lumesis had access.

7. All computer artifacts[8] for any computer device (including laptops, desk computers, and tablets) issued to Pendolino by Lumesis, including the Dell XPS desk top computer, serial number H080KB2, sufficient to show whether any DAC Documents, data or information has resided on, has been transmitted to or from, has been stored for any period of time on or in, or has been deleted from any such computer device, or any component or part thereof.

8. All Documents that constitute, reflect or relate to communications between Pendolino and Stifel Financial Corp. or any affiliate of Stifel Financial Corp. (collectively, "Stifel") or any person or entity acting for Stifel, including Mary McPike.

9. All Documents concerning efforts by Pendolino or Lumesis to develop a Summary Findings Page or other record that serves the same or an equivalent function or object as the DAC Summary Findings Page.

10. All Documents evidencing discussions between Lumesis and Pendolino concerning the recruitment of, relationship with or employment of Pendolino by Lumesis.

---

[8] DAC did not define the term "computer artifacts" as used in the subpoena (Doc. 67 at 16). In his declaration, DAC's expert said:

> The version of the Windows in use on the laptop does not leave artifacts when a file is copied from the laptop to an attached USB device. This is in contrast to when a computer is used to browse or open folders resident on a USB device. When a computer is used to take data off of a USB device it leaves traces, when a computer is used to move data onto a USB device it does not leave traces. For example, when a file is dragged and dropped to a USB drive from a computer using Windows Explorer no forensic artifacts are created. If that file, or any other file resident on the USB device, is then accessed from the computer forensic artifacts are created. Analysis to determine if files were copied from the hard drive or network shares to the USB device using the laptop alone are therefore inconclusive.

(Doc. 5, ¶ 8). It is not clear whether these are the "artifacts" sought by the subpoena. According to the Court's own research, "computer artifacts" are "one of many kinds of tangible by-products produced during the development of software. Some artifacts …help describe the function, architecture, and design of software. Other artifacts are concerned with the process of development itself–such as project plans, business cases, and risk assessments." https://en.wikipedia.org/wiki/Artifact_(software_development).

11. All Documents that constitute, reflect or relate to the employment of Pendolino by Lumesis.

12. All Documents that constitute, reflect or relate to the identity of any DAC client or client list disclosed to or discussed with Lumesis by Pendolino.

13. All Documents that constitute, reflect or relate to any policy or practice of Lumesis pertaining to or governing use by Lumesis employees of any computer issued to such employee by Lumesis or governing use or access to any Lumesis email system, database, shared network drive, cloud network interface, storage provider, electronic interface or storage medium to which Pendolino had access.

14. A forensic image of any cellphone, tablet, physical storage device, or device or program used to access cloud storage, that was used to copy, download, transmit, receive, open or store any DAC Documents.

15. Any DAC document or information transmitted or stored for any period of time to the Lumesis secure Google drive on the cloud.

16. All Documents concerning or containing information created by, in any way communicated or disseminated by, or ever belonging to, DAC, including without limitation: (i) client contracts; (ii) marketing information; (iii) client request for reviews and the summary page of results or other work papers documenting the results of the summary findings; (iv) financial information, including but not limited to profitability and cash flow data; (v) DAC employee compensation and bonus data; and (vi) any other information transferred to you from DAC.

17. All Documents concerning the use, transfer, communication, deletion or destruction of any Documents covered by this Subpoena.

18. All Documents or information relating to DAC resulting from a search of the Outlook account, including any sent or received mail, of the Dell XPS desk top computer, serial number H080KB2, issued by Lumesis to Pendolino using each of the following search terms:

- DAC
- digital assurance
- summary
- client
- Stifel

- McPike
- Raymond James

19. All Documents that constitute, reflect or relate to communications between Pendolino or Lumesis and U.S. Bank from October 1, 2016 through November 30, 2016.

(Doc. 68 at 2, 6-12; Doc. 68-1 at 9-19).

The President and CEO of Lumesis, has submitted a declaration stating that compliance with the subpoena would require the company to search every computer for every Lumesis employee, across multiple platforms (Doc. 67-4 at ¶ 19). He says that compliance would also require the disclosure of Lumesis's trade secrets to DAC and invade the privacy of Lumesis employees (Id.). DAC has attempted to alleviate Lumesis' confidentiality and privacy concerns through the making of a confidentiality agreement between it, Pendolino, and Lumesis (Doc. 73 at 3). The Court is unaware of the status of this agreement. DAC also argues that as the leader in its field, it does not want or need information from Lumesis (Id. at 8).

A computer forensic expert hired by Lumesis has opined that because DAC has not provided a specific way to identify the documents it seeks, it is impossible to:

> [D]efine, refine, or limit the Data Collection or volume of production by document type, advanced key word searches, indexing, sampling, de-duplication, predictive coding, and other strategies to actually be able to find relevant responsive Data that is non-privileged and does not contain Lumesis Information or Lumesis Trade Secrets.

(Doc. 67-8 at ¶ 8). The expert says that because Lumesis operates "on the cloud," the subpoena will require "the imaging not only of specific identifiable computer(s) and devices, but *all* Lumesis platforms, network servers and cloud servers." (Id. at ¶ 10) (Emphasis in original). According to the expert:

> Conducting complete e-discovery and forensic imaging as required by the Subpoena will likely result in at least a minimum of 150 or more hours of Data Collection and Data Processing *alone*, for which HaystackID's fees would be at least $75,000, exclusive of imaging, global key word searching, and document hosting for review and litigation support services.

(Id. at ¶ 11) (Emphasis in original, footnote omitted). The expert also states that "[d]ocument hosting for review and litigation support services could result in at least another $20,000-$25,000 in fees, depending on the volume of Data Collection." (Id. at ¶ 14).

Lumesis objected to every category of documents in the subpoena (Doc. 67 at 5; Doc. 73 at 2). This resulted in discussions between counsel concerning what Lumesis would be willing to produce (Id.). During a conversation on June 16, 2017, an attorney for DAC allegedly said he had obtained "access" to Lumesis' underwriter platform, and was in possession of documents showing what the underwriter platform "does." (Doc. 67 at 5). The attorney allegedly said he had obtained this information "properly," but would not say how he got it (Id.). The attorney in question denies making these statements (Doc. 73 at 4-5; Doc. 73-6). He also represents that he and DAC do not have access to Lumesis' DIVER platform, and that the information DAC has concerning the DIVER report was received lawfully in the ordinary course of business (Doc. 73 at 4). Lumesis contends that counsel did make these statements and as a result, for some period of time it took the position that even if the parties signed an agreement to protect the confidentiality of information provided in discovery, the DAC lawyer in question and his firm should not be given access to Lumesis' trade secrets and other information (Doc. 72 at 6). This no

longer appears to be an issue but if the Court is wrong, and resolution is required, the Court will hold an evidentiary hearing on the matter.[9]

During the same June 16 telephone conversation, attorneys for Lumesis offered to search their client's computer system to determine if any of DAC's documents allegedly accessed by Pendolino are on the system (Doc. 67 at 6). To make this search, they asked for the MD5 hash value identifiers for each of the allegedly misappropriated documents (Id.). A "hash value," or "hash coding" is: "A mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified. Common hash algorithms include MD5 …." See The Sedona Conference Glossary: E-Discovery and Digital Information Management (Fourth Edition). Lumesis' computer expert states that the MD5 hash value for a document is the same for all copies of the original document (Doc. 67-8 at ¶ 6). "Thus, one can do a search for the identical document using the same MD5 hashtag. In other words, if DAC ran the MD5 algorithm on each of the DAC Documents it alleges were misappropriated, and provided the resulting MD#5's to Lumesis, Lumesis could run searches of Pendolino's computer to locate them." (Id.). The Court understands that because this method identifies the specific documents to be searched for, it reduces the time and expense of a search. DAC has not provided any MD5 hash values to Lumesis (Doc. 67 at 6).

On June 27, 2017 Lumesis notified DAC that it had located a page it calls "DAC Bond findings" dated January 6, 2016 (Doc. 67-6 at 4). Lumesis represents that it received the document in an email from one of its clients, and that it has not used the

[9] When counsel do not trust one another, it is the clients who foot the bill. They will now pay the attorneys to engage in more detailed communications and document every word and deed. This distrust will also be an impediment to compromise and settlement.

document (Id.). Lumesis has produced a copy of the email thread to substantiate this assertion (Id.). DAC has identified the document as a copy of one of its proprietary summary pages (Doc. 73-6 at 7).

In its proposed amended complaint, DAC alleges "[u]pon information and belief, the Summary Findings Page developed by Lumesis as part of its 'DIVER' platform is substantially similar to the DAC Summary Findings Page and follows the same presentation format in significant respects. Upon information and belief, this new Summary Findings Page is substantially different from products offered by Lumesis prior to November 2016." (Doc. 75 at ¶ 67).

On July 28 Lumesis served its second amended response to the subpoena (Doc. 68-1). In this response, it agreed to provide Pendolino's employment agreement, and to "conduct and provide DAC with the results of a search of the Outlook account for the Dell XPS desktop computer, serial number H080KB2 for the terms 'DAC' and 'Digital Assurance.'" (Id. at 18). However, this information has not been provided to DAC (Doc. 68 at 13). Lumesis has advised DAC that it does not have any documents responsive to subpoena category 12 and therefore, DAC does not seek to compel that category of the subpoena (Doc. 68 at 5, n. 5).

Lumesis argues that the motion to compel should be denied because counsel for DAC did not comply with Local Rule 3.01(g) before the motion was filed[10] (Doc. 72 at 7-9) and that counsel for DAC "materially misrepresents the content of" a telephone

[10] Local Rule 3.01(g) provides that before filing most motions in a civil case, the moving party shall confer with the opposing party in a good faith effort to resolve the issues raised by the motion, and then file with the motion a statement certifying that the moving party has conferred with the opposing party, and that the parties have been unable to agree on the resolution of the motion. The term "confer" in Rule 3.01(g) requires a substantive conversation in person or by telephone in a good faith effort to resolve the motion without court action. Counsel who merely "attempt" to confer have not "conferred." See Local Rule 3.01(g). The Court will deny motions that fail to include an appropriate Rule 3.01(g) certificate.

conference between counsel (Id. at 9). DAC disputes these contentions and lawyers on both sides have filed declarations setting forth their recollections of what happened (Docs. 72-1, 73-7). Local Rule 3.01(g) applies to parties and Lumesis was not a party when the motion to compel was filed.[11] Still, it is recommended that "in most cases, the party issuing the subpoena and the non-party responding to the subpoena should discuss, in advance, the same issues a party would discuss with an opposing party before commencing discovery of [electronically stored information]." Middle District Discovery (2015) at 26. While DAC's motion to compel is not subject to denial for failure to comply with Rule 3.01(g), allegations that anyone has made a material misrepresentation to the Court are serious. If further claims of misrepresentation are made, then the Court will hold an evidentiary hearing where everyone with knowledge will testify and the Court will decide their credibility, and enter appropriate orders.

Lumesis alleges that DAC served the subpoena to harass the company and obtain its trade secrets (Doc. 67). It complains that the subpoena is unreasonable, unduly burdensome, and not proportional to the needs of the case (Id., at 8-12). Lumesis argues that DAC has no evidence to support its claims against Pendolino and is proceeding solely on the basis of speculation (Id. at 12). It also objects that the subpoena: (1) is overly broad; (2) the information sought is not identified with reasonable particularity; (3) compliance would require the disclosure of Lumesis' proprietary information to its competitor; (4) compliance would be costly and inconvenient; (5) the subpoena seeks information that is not related to the claims that have been asserted against Pendolino; (6) some of the information sought is subject to confidentiality and non-disclosure

[11] Whether DAC has served Lumesis is unknown.

obligations; (7) the information is more easily obtained from Pendolino; (8) the subpoena seeks information that predates Lumesis' employment of Pendolino; (9) Lumesis has already produced the sole document it is aware of that is in its possession; (10) DAC has not defined some of the terminology used in the subpoena; and (11) the subpoena seeks information already in DAC's possession (Doc. 68-1). On these grounds, Lumesis asks the Court to quash the subpoena or, in the alternative, issue a protective order.

DAC argues that Lumesis' motion should be denied and its motion to compel should be granted. It maintains that it "took care to narrowly tailor" the subpoena to only seek: "(i) DAC materials that were provided to Lumesis by Pendolino, (ii) DAC materials placed onto Lumesis's network or devices by Pendolino, (iii) DAC materials provided to Lumesis by a third party who received them from, or acting through a connection with, Pendolino, (iv) data and information concerning Pendolino's use of Lumesis's computer and network system, and (v) documents concerning Pendolino's and Lumesis's communications concerning Pendolino's employment with Lumesis." (Doc. 73 at 5, 9). DAC argues that Lumesis' objections are for the most part, improper boilerplate of the sort the Court routinely rejects[12] (Doc. 68 at 5-16). It contends that the information it seeks is relevant to this controversy and that the subpoena was necessitated by Pendolino's insistence that the information can only be obtained from Lumesis (Doc. 68 at 2-3, 5-16). And, now that the Court has granted the motion for leave to amend, DAC is adding Lumesis as a party to this action (Doc. 75).

Legal Standards

"The overall purpose of discovery under the Federal Rules is to require the

[12] See, Polycarpe v. Seterus, Inc., No. 6:16-cv-1606-Orl-37TBS, 2017 WL 2257571, at *1-2 (M.D. Fla. May 23, 2017).

disclosure of all relevant information so that the ultimate resolution of disputed issues in any civil action may be based on a full and accurate understanding of the true facts, and therefore embody a fair and just result." Oliver v. City of Orlando, No. 6:06-cv-1671-Orl-31DAB, 2007 WL 3232227, at *2 (M.D. Fla. Oct. 31, 2007) (in turn citing United States v. Proctor & Gamble Co., 356 U.S. 677, 682 (1958)).

Pursuant to Federal Rule of Civil Procedure 45, a party may subpoena from a nonparty, documents, electronically stored information ("ESI"), or tangible things in the non–party's possession, custody, or control for inspection, copying, testing, or sampling. FED. R. CIV. P. 45(a)(1)(A)(iii), (a)(1)(D). The scope of discovery under Rule 45 is the same as the scope of discovery under Federal Rule of Civil Procedure 26. Baptiste v. Ctrs., Inc., No. 5:13-civ-71-Oc-22PRL, 2013 WL 3196758, at *2 (M.D. Fla. June 21, 2013); see also Chambers v. Sygma Network, Inc., Case No. 6:12-cv-1802-ORL-37TBS, 2013 WL 1775046, at *3 (M.D. Fla. April 25, 2013) (quoting Rule 26(b)(1) and applying to a Rule 45 subpoena dispute); Madeline LLC v. Street, No. 09-80705-MC, 2009 WL 1563526, at *1 (S.D. Fla. June 3, 2009) ("Rule 45 must be read in conjunction with [Rule] 26, because the latter rule 'clearly defines the scope of discovery for all discovery devices.'") (citations omitted). Under Rule 26, unless the Court enters an order limiting discovery,

> Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering 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. Information within this scope of discovery need not be admissible in evidence to be discoverable.

FED. R. CIV. P. 26(b)(1).

Rule 26's requirement that discovery be relevant "'signals to the court that it has the authority to confine discovery to the claims and defenses asserted in the pleadings, and signals to the parties that they have no entitlement to discovery to develop new claims or defenses that are not already identified in the pleadings.'" Builders Flooring Connection, LLC v. Brown Chambless Architects, No. 2:11CV373-MHT, 2014 WL 1765102, at *1 (M.D. Ala. May 1, 2014) (quoting GAP Report of Advisory Committee to 2000 amendments to Rule 26). "As the Advisory Committee Notes say, '[t]he Committee intends that the parties and the court focus on the actual claims and defenses involved in the action.'" Liese v. Indian River Cty. Hosp. Dist., 701 F.3d 334, 355 (11th Cir. 2012) (quoting the GAP Report). On a motion to compel, the party desiring to enforce a subpoena bears the burden of demonstrating that the information it seeks is relevant. Fadalla v. Life Auto. Prods., Inc., 258 F.R.D. 501, 504 (M.D. Fla. 2007); Connectus LLC v. Ampush Media, Inc., Case No. 8:16-mc-00159-VMC-JSS, 2017 WL 385758, *2 (M.D. Fla Jan. 27, 2017).

Rule 26 also requires that discovery be proportional to the needs of the case. In making this determination, the court is guided by the non-exclusive list of factors in Rule 26(b)(1). Graham & Co., LLC v. Liberty Mut. Fire Ins. Co., No. 2:14-cv-2148-JHH, 2016 WL 1319697, at *3 (N.D. Ala. April 5, 2016). "Any application of the proportionality factors must start with the actual claims and defenses in the case, and a consideration of how and to what degree the requested discovery bears on those claims and defenses." Id. (quoting Witt v. GC Servs. Ltd. P'ship, 307 F.R.D. 554, 569 (D. Colo. 2014)).

In discussing proportionality and the discovery of ESI, the Middle District's Discovery Handbook cites the following principles of proportionality published by The Sedona Conference:

> 1. The burdens and costs of preserving relevant electronically stored information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation.
>
> 2. Discovery should focus on the needs of the case and generally be obtained from the most convenient, least burdensome and least expensive resource.
>
> 3. Undue burden, expense, or delay resulting from a party's action or inaction should be weighed against that party.
>
> 4. The application of proportionality should be based on information rather than speculation.
>
> 5. Nonmonetary factors should be considered in the proportionality analysis.
>
> 6. Technologies to reduce cost and burden should be considered in the proportionality analysis.

Middle District Discovery (2015) at 24 (citing The Sedona Conference: Commentary on Proportionality in Electronic Discovery, 11 Sedona Conf. J. 289 (2010)).

A nonparty may object and move to quash a subpoena on the ground that it imposes an undue burden. FED. R. CIV. P. 45(d)(3)(A)(iv). The burden is on the nonparty to make this showing. Fadalla, 258 F.R.D. at 504; Malibu Media, LLC v. Doe, No. 8:14-cv-2352-T-36AEP, 2015 WL 574274, at *3 (M.D. Fla. Feb. 11, 2015) (citing Indep. Mktg. Group, Inc. v. Keen, No. 3:11-cv-447-J-25MCR, 2012 WL 512948, at *2 (M.D. Fla. Feb. 16, 2012)). In deciding whether a subpoena imposes an undue burden courts balance the requesting party's need for the discovery against the burden imposed on the subpoenaed party. Fadalla, 258 F.R.D. at 504. Factors courts consider when performing this balancing test include: (1) the relevance of the information requested; (2) the need of the requesting

party for its production; (3) the breadth of the request for production; (4) the time period covered by the subpoena; (5) the particularity with which the subpoena describes the requested production; and (6) the burden imposed on the subpoenaed party. Id.; Schaaf v. SmithKline Beecham Corp., No. 3:06-cv-120-J-25TEM, 2006 WL 2246146, *2 (M.D. Fla. Aug. 4, 2006). "[T]he status of the person as a non-party is a factor often weighing against disclosure." Schaaf, 2006 WL 2246146, at *2; FED. R. CIV. P. 45(d)(3)(A)(iii)-(iv), (B)(i).

Parties and nonparties can move the court for the entry of a protective order to "protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense" by, among other things, "forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters." FED. R. CIV. P. 26(c)(1)(D). On a motion for the entry of a protective order the moving party has the burden to show good cause. In re Deutsche Bank Trust Co., 605 F.3d 1373, 1378 (Fed. Cir. 2010). Good cause requires a specific demonstration of facts to support the motion; conclusory statements about need and harm are not sufficient. Baratta v. Homeland Housewares, LLC, 242 F.R.D. 641, 642 (S.D. Fla. 2007); see also Resolution Trust Corp. v. Worldwide Ins. Mngm't Corp., 147 F.R.D. 125, 127 (N.D. Tex. 1992); Blum v. Schlegel, 150 F.R.D. 38, 41 (W.D.N.Y. 1993). "If a sufficient showing of good cause is made, the burden then shifts to the non-moving party to show why relief should still not be granted, either because of undue prejudice or the importance of the discovery at issue." New World Network, Ltd. v. M/V Norwegian Sea, No. 05-22916-CIV-JORDAN/TORRES, 2007 U.S. Dist. LEXIS 25731, at * 3 (S.D. Fla. April 6, 2007).

Although good cause is the standard under Rule 26(c), courts in the Eleventh Circuit "have superimposed a somewhat more demanding balancing of interests

approach to the Rule." Farnsworth v. Proctor & Gamble Co., 758 F.2d 1545, 1547 (11th Cir. 1985); Cf. Ekokotu v. Fed. Express Corp., 408 F. App'x 331, 336 (11th Cir. 2011) (citing McCarthy v. Barnett Bank of Polk Cnty., 876 F.2d 89, 91 (11th Cir. 1989)). This requires the court to balance the non-moving party's interest in obtaining the discovery against the moving party's interest that the discovery not be had.

Discussion

In discovery, relevance is "construed broadly to encompass any matter that bears on" the claims and defenses asserted in the case. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351, 98 S.Ct. 2380, 57 L.Ed.2d 253 (1978). Whether Lumesis is in possession of DAC's confidential and proprietary information is relevant to DAC's claims made in the original and amended complaints. If Lumesis is in possession of DAC's confidential information, then how it was obtained is also relevant.

But, is the scope of discovery demanded by the subpoena proportional to the needs of the case? "The parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes." Advisory Committee Notes, 2015 Amendment. When, as here, a discovery dispute arises, "[t]he court's responsibility, using all the information provided by the parties, is to consider these and all the other factors in reaching a case-specific determination of the appropriate scope of discovery." Id.

Lumesis has already made a search and located a single page that is responsive to the subpoena. DAC does not accept the results of this search and wants what in pre-ESI days would amount to entering Lumesis' offices and looking at every item on every desk and in every drawer and cabinet. This is extraordinary, particularly in light of the limited factual support for such a significant intrusion.

The Court is unaware of any witness who will testify that they saw Pendolino steal anything from DAC. There is also no digital trail or "artifacts" showing that Pendolino, or anyone else for that matter, copied DAC's confidential information and then gave it to Lumesis.

One DAC client moved its business to Lumesis. Whether that happened before or after Pendolino changed employers is in dispute and whether this even matters is debatable. In its amended complaint, DAC alleges that the client said "the move to Lumesis was being done for purely economic reasons." (Doc. 75 at ¶ 66). If this is true, then the loss of this client may have nothing to do with DAC's allegations against Pendolino and Lumesis.

Lumesis has solicited one or more of DAC's other clients. In the absence of improper methods (the Court is unaware of any), there is nothing wrong with competitors pursuing one another's clients. That is what competition is about.

DAC heard that Lumesis was developing its own summary page and, in its amended complaint alleges, on "information and belief," that after November 2016, Lumesis began utilizing a page that is very similar to DAC's summary page (Id. at ¶ 67). Missing are facts linking Pendolino to the development of Lumesis' new page, and facts showing that Lumesis made unlawful use of DAC's proprietary information to develop the new page.

If Lumesis obtained DAC's confidential information in November, 2016, and has now taken advantage of it for approximately ten months, the Court would expect DAC to

point to specific, significant damages it has incurred. But, DAC has not suggested an amount in controversy and complains about the loss of a single client.[13]

It appears that to succeed on the merits, DAC must discover Pendolino and/or Lumesis in possession of its confidential information. All of this suggests to the Court that DAC is proceeding largely on the basis of speculation as opposed to information.

Still, the issues at stake are important. Unless trade secrets are protected, the motivation to innovate is chilled. This makes the protection of trade secrets a global concern that is reflected in the statutes under which DAC sues Pendolino and Lumesis.

In all likelihood discovery in this case will be asymmetrical. By this the Court means that Pendolino and Lumesis probably control significantly more relevant information than DAC has. While proportionality requires that all parties have access to relevant information, the concept of proportionality exists to prevent one party, in this case DAC, from leveraging that asymmetry to obtain a tactical advantage over the Defendants. By like token, Defendants should not be permitted to leverage their access to information by employing dilatory tactics to withhold appropriate discovery from DAC.

Looking at this dispute objectively, it is reasonable for Lumesis to run MD5 hash value identifiers for key documents, and to search key words to determine whether any of DAC's confidential information resides in its systems. Any greater search, particularly one that may cost as much as $100,000 and reveal Lumsis' confidential information is disproportionate to the needs of the case. Even if the Court were to find otherwise, it would still not enforce every category in the subpoena because some ("artifacts" for example), do not describe what is being sought with the requisite particularity.

[13] The Court may also consider the value of the injunctive relief DAC seeks in evaluating the amount in controversy but that does not change the point the Court is attempting to make.

Now, the motion to quash is **GRANTED** and DAC's subpoena served on Lumesis is **QUASHED**. Lumesis's alternative motion for a protective order is **DENIED as moot**. DAC's amended motion to compel is **DENIED**.

DONE and **ORDERED** in Orlando, Florida on September 29, 2017.

THOMAS B. SMITH
United States Magistrate Judge

Copies furnished to Counsel of Record