

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF INDIANA  
INDIANAPOLIS DIVISION

ONEAMERICA FINANCIAL	)	
PARTNERS, INC.,	)	
	)	
Plaintiff,	)	
	)	No. 1:15-cv-01534-TWP-DKL
vs.	)	
	)	
T-SYSTEMS NORTH AMERICA, INC.,	)	
<i>et al.</i> ,	)	
	)	
Defendants.	)	

*Entry on Plaintiff's Motion to Maintain Certain Portions of Documents Under Seal [doc. 41] and TSNA's Motion to Seal Its Motion to Bifurcate and for Speedy Trial on Count III of Its Counterclaim [doc. 56]*

This cause comes before the Court on *Plaintiff's Motion to Maintain Certain Portions of Documents Under Seal [doc. 41] and TSNA's Motion to Seal Its Motion to Bifurcate and for Speedy Trial on Count III of Its Counterclaim [doc. 56]*. District Judge Tanya Walton Pratt referred the motions to the undersigned for ruling. Having considered the motions and supporting materials, the Court decides as follows.

*Background*

OneAmerica Financial Partners, Inc. brought this action against T-Systems North America, Inc. ("TSNA"), and T-Systems International GmbH for breach of contract, fraudulent inducement, fraud, negligence, and promissory estoppel and for breach of guaranty against T-Systems International. Several years ago, OneAmerica decided to outsource certain Information Technology ("IT") services. It hired technology

consultants to develop a Request for Proposal for Information Technology Infrastructure Services (“RFP”). OneAmerica and TSNA executed a Master Information Technology Services Agreement (“MITSA”), pursuant to which TSNA was to provide certain IT services and equipment to OneAmerica. In this action, OneAmerica alleges that TSNA failed to provide the high quality IT services as promised under the MITSA. TSNA has counterclaimed for breach of contract, fraud, and declaratory relief.

OneAmerica moves to maintain under seal certain portions of the RFP [docs. 6-1 through 6-4], the MITSA [docs. 7-1 through 7-6], *T-Systems North America, Inc.’s Answer, Affirmative Defenses, Reliance on Jury Demand, and Counter-Complaint* (“*Counter-Complaint*”) [docs. 19 and 19-1], and corresponding portions of *OneAmerica Financial Partner, Inc.’s Un-Redacted Answer and Affirmative Defenses to T-Systems North America, Inc.’s Counter-Complaint and Jury Demand* (“*Answer to Counter-Complaint*”) [doc. 33]. Plaintiff states that it requests “the Court to maintain under seal only the contents which identify specific details about [its] software, applications, hardware, vendors, regional locations, and Information Technology (“IT”) policies and procedures.” [*Pl.’s Mot. Maintain Certain Portions of Docs. Under Seal*, doc. 41 at 1.] It argues good cause exists “to maintain these portions of the documents under seal in order to prevent a potential data breach of OneAmerica’s IT systems.” [*Id.*] Given the voluminous filings at issue (in excess of 1,000 pages), OneAmerica did not file copies of the documents with the portions at issue redacted, but states that it will do so at the Court’s direction.

OneAmerica submits that it is not necessary to disclose specific information about its IT systems to the public at this stage of the litigation because such information “will

not materially assist the public in understanding and monitoring” the case. [*Pl.’s Br. Supp. Mot. Maintain Certain Portions of Docs. Under Seal*, doc. 42 at 2.] Those portions of the documents that are disclosed to the public, it argues, will allow interested parties to know who is using the courts, to understand the judicial decisions in the case, and to monitor the Court’s resolution of the issues. [*Id.* at 5.] If the claims, defenses, or counterclaims focus on specific software or hardware, OneAmerica argues that the disclosure to the public of information relating to such software or hardware can be addressed at that time, but disclosure of details is unnecessary at this early stage of the litigation. [*Id.* at 2.]

The Court previously denied OneAmerica’s motion to seal the RFP and MITSA in their entireties and to seal a portion of the Counter-Complaint. However, the Court allowed OneAmerica to attempt to make a sufficient showing that the documents and portions thereof should be maintained under seal. [*See* doc. 31].

OneAmerica filed two affidavits in support of its current motion, the affidavit of Kevin Weston, Vice President of IT Infrastructure Resource Management at OneAmerica Financial Partners, Inc. [doc. 42-1] and the affidavit of Yaniv Schiff, Director of Digital Forensics at Forensicon, Inc. [doc. 42-2]. Weston states that “there is good cause” to maintain portions of the documents under seal “because they reveal sensitive details about OneAmerica’s IT infrastructure and IT systems that increase the risk of a data breach to OneAmerica’s IT systems.” [Doc. 42-1 at 2, ¶ 6.] He continues: “The portions of information that OneAmerica must maintain under seal are those portions which identify the specific software and applications that OneAmerica utilizes, specific hardware that OneAmerica uses, OneAmerica’s vendors, OneAmerica’s regional office

locations, and the details of OneAmerica’s IT operations, policies and procedures.” [Id. ¶ 7.] According to Weston, “each reveals vulnerabilities and access points for hackers to perpetrate a data breach.” [Id. at 3, ¶ 7.] The software and applications are identified by name in portions of the MITSA, RFP, and *Counter-Complaint*. [Id. at 3, ¶ 8.] With knowledge of “specific hardware information such as vendor, product name, serial number, and model,” Weston states, “a hacker can more easily perpetrate a ‘social engineering’ hack whereby the hacker is able to trick or manipulate a OneAmerica employee into performing actions or divulging confidential information to the hacker” and with knowledge of “precise devices and models” of hardware, a hacker “could exploit known vulnerabilities in such hardware published in various locations on the so-called ‘Dark Web.’” [Id. ¶ 9.]

Weston asserts that it is important not to disclose the identity of OneAmerica’s IT vendors and contacts because hackers could exploit vulnerabilities there to gain access to OneAmerica’s systems. [Id. at 4, ¶ 10.] He states that the list of OneAmerica’s regional offices should not be revealed, specially “in tandem with the identities of the specific software, applications, and hardware operating at those locations” because hackers could use that information to “target regional corporate locations as remote access points to breach larger corporate networks and enterprise data centers.” [Id. ¶ 11.] Portions of the regional locations may be perceived to have less security than OneAmerica’s headquarters and primary enterprise data centers, and thus may be “likely hacker targets.” [Id.] Furthermore, according to Weston, the details of OneAmerica’s “IP operations, policies, and procedures” included in portions of the MITSA “disclose

OneAmerica’s highly confidential IT information, including specific passwords, system commands, and recovery processes.” [Id. ¶ 12.] That information would give hackers insight into OneAmerica’s recovery processes, which could reveal vulnerabilities. [Id.]

OneAmerica argues that disclosure of the above information “could assist a hacker in exploiting vulnerabilities in [its] system to perpetrate a data breach similar to the recent Anthem breach subjecting millions of people’s confidential personal information to exposure.” [Id. at 5, ¶ 13.] The threat of data breaches is increased, Weston submits, “by the fact that TSNA’s defenses and counter-claims are based in part on allegations that OneAmerica’s IT systems are outdated and antiquated.” [Id. ¶ 14.] And because it is in the midst “of a massive transition ... to a new IT infrastructure service provider,” Plaintiff asserts that it is unusually vulnerable to a data breach at this time. [Id. ¶ 15.] Weston states that a data breach “would affect hundreds of thousands of OneAmerica customers by putting their confidential personal and financial information at risk,” including their “personally identifiable information such as social security numbers, account numbers, and other identification numbers” and “could also expose OneAmerica’s proprietary business data.” [Id. ¶ 16.]

In addition to being Director of Digital Forensics, Schiff is a Certified Computer Examiner and a member of the High Technology Crime Investigation Association and International Association of Computer Investigative Specialists. He has served as an adjunct professor teaching computer forensics at Loyola University in Chicago, Illinois. [Doc. 42-2 at 1 ¶¶ 2-4.] Schiff has not reviewed the RFP or MITSA, but states that he has “a general understanding of the topics in those documents” as well as in TSNA’s

Counter-Complaint and OneAmerica's Answer thereto. [*Id.* at 2, ¶ 6.] He asserts that certain types of information that OneAmerica seeks to maintain under seal could assist a hacker to breach OneAmerica's IT systems or to obtain confidential information through social engineering. [*Id.* at 2, ¶ 7.] In particular, "information identifying OneAmerica's software, applications, hardware, contractors and IT policies and procedures could assist hackers in breaching [its] IT systems." [*Id.*; *see also id.* at 2-4, ¶¶ 8-11, 13.] Further, disclosure of OneAmerica's regional locations, including non-office regional locations such as data centers, which are not typically widely known or generally available to the public, could assist hackers in breaching OneAmerica's IT systems. [*Id.* at 4, ¶ 12.]

According to Schiff, OneAmerica "is already a prime target for hackers because it is a financial institution holding personally identifiable and confidential financial information for hundreds of thousands of customers" and it is "at an increased risk" for being targeted for a data breach because: (1) Defendants have alleged that its IT systems are antiquated and need to be replaced, and (2) it is presently transitioning to a new IT service provider, "which could make it more difficult to detect and thwart a data breach." [*Id.* at 4-5, ¶ 14.] Finally, Schiff suggests that the risk is increased because information that a hacker would otherwise have to spend time and effort gathering to assess OneAmerica's IT system's security is "provide[d] in a single source information." [*Id.* at 5, ¶ 14.] Both Weston and Schiff state essentially that one cannot know how a hacker would execute a breach of OneAmerica's IT systems. [*Id.* at 2, ¶ 7; doc. 42-1 at 2-3, ¶ 7.]

TSNA filed its motion to seal in order to provide OneAmerica with an opportunity to meet the good cause standard for maintaining under seal certain information

contained in TSNA's motion to bifurcate and for speedy trial as well as Exhibit 1 attached to the motion to bifurcate. [See *Sealed T-Sys. N. Am., Inc.'s Mot. Bifurcate & for Speedy Trial on Count III of its Counterclaim*, doc. 55; *Billing Resolution, Termination, and Asset Purchase Agreement and Amendment to the Master Information Technology Services Agreement* ("Billing Agreement"), doc. 55-1.] TSNA disagrees with OneAmerica's position that certain agreements and information should be maintained under seal.

#### *Discussion*

"Documents that affect the disposition of federal litigation are presumptively open to public view ... unless a statute, rule, or privilege justifies confidentiality." *In re Specht*, 622 F.3d 697, 701 (7th Cir. 2010). The "right of public access ... enable[s] interested members of the public ... to know who [is] using the courts, to understand judicial decisions, and to monitor the judiciary's performance of its duties." *Goesel v. Boley Int'l (H.K.) Ltd.*, 738 F.3d 831, 833 (7th Cir. 2013) (chambers opinion). Courts recognize limited matters subject to seal, including trade secrets and other confidential commercial information. See *United States v. Sanford-Brown, Ltd.*, 788 F.3d 696, 712 (7th Cir. 2015); Fed. R. Civ. P. 26(c)(1)(G). If material may be subject to seal, then the court weighs two competing interests: "the moving party's interest in privacy and the public's interest in transparency." *Sanford-Brown*, 788 F.3d at 712.

A court may shield a document or portion thereof from the public only if there is good cause to do so. See, e.g., *Bond v. Utreras*, 585 F.3d 1061, 1074 (7th Cir. 2009); *Citizens First Nat'l Bank v. Cincinnati Ins. Co.*, 178 F.3d 943, 945 (7th Cir. 1999). If "good cause is shown, parties may seal documents to protect their own interests or interests of third

parties.” *Ratajczak v. Beazley Sols. Ltd.*, No. 13-C-045, 2013 WL 6817308, at \*1 (E.D. Wis. Dec. 23, 2013) (citing, *ineter alia*, *Bank of Am., N.A. v. First Mut. Bancorp of Ill.*, No. 09-5108, 2010 WL 2921845, at \*1 (N.D .Ill. July 22, 2010) (“The court will protect financial information about ‘third party borrowers,’ that is, people and entities who are not parties to this case.”)).

A. *OneAmerica’s Motion to Seal*

OneAmerica seeks to maintain under seal portions of certain documents that identify details about its (1) software, applications, or hardware, (2) vendors, (3) regional locations, and (4) IT policies and procedures. In responding to OneAmerica’s motion, TSNA first contends that Plaintiff failed to identify any statute, rule, privilege, or legal citation to justify sealing the portions of the documents at issue. While OneAmerica’s motion and supporting brief may have been deficient in this regard, its reply brief has cited appropriate authority. [See *Pl.’s Reply*, doc. 52 at 3-5 (citing cases).] Courts have concluded that concerns about hackers and a cyber attack justified sealing information about a company’s IT systems. See, e.g., *Music Grp. Macao Comm. Offshore Ltd. v. Foote*, No. 14-CV-03078 JSC, 2015 WL 3993147, at \*5-6 (N.D. Cal. June 30, 2015) (finding a compelling reason to seal portions of exhibit discussing plaintiff’s network infrastructure and security systems); *EON Corp IP Holdings LLC v. Cisco Sys. Inc.*, No. 12-CV-01011-JST, 2014 WL 1017514, at \*2 (N.D. Cal. Mar. 11, 2014) (finding compelling reasons to seal portion of documents that disclose “confidential technology, product configurations, security features, and network configurations”); *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 WL 5366963, at \*3 (N.D .Cal. Sept. 25, 2013) (sealing information about

how users' interactions with the Gmail system effect the transmission of messages based on Google's assertions that "hackers and spammers could use this information to circumvent Google's anti-virus and anti-spam mechanisms"); *Metavante Corp. v. Emigrant Sav. Bank*, No. 05-CV-1221, 2009 WL 637165, at \*1 (E.D. Wis. Mar. 11, 2009) (granting motion to seal email that appeared to contain "confidential information on specific types of software used by [defendant]").

TSNA argues that OneAmerica failed to offer an explanation as to how a hacker would use any specific information to undertake a data breach. While Plaintiff did not offer a specific explanation, both Weston and Schiff essentially state that it is impossible to predict what information would be most useful for a hacker or how a hacker would execute a breach of OneAmerica's IT systems. TSNA criticizes Schiff for not reading the RFP or MITSA, which he did not. Nonetheless, he states that he is familiar with the topics in those documents, the *Counter-Complaint*, and the *Answer* thereto, and that the types of information that Plaintiff seeks to protect could assist a hacker to breach OneAmerica's IT systems or obtain confidential information. The Court credits his opinions.

*Zahran v. Trans Union Corp.*, No. 01-cv-1700, 2002 WL 31010822, at \*3 (N.D. Ill. Sept. 9, 2002), TSNA maintains, supports its position that Plaintiff has failed to justify the sealing of any document. In that case the defendant moved the court to enter a protective order and to seal certain exhibits and statements in the pleadings, which it argued contained trade secrets and other confidential commercial information. *Id.* at \*1. The exhibits at issue contained portions of the defendant's consumer relations center Dispute Training Guide and subscriber agreements entered into between the defendant and

several of its customers. *Id.* at \*2. The defendant argued that anyone who gained unauthorized access to its consumer relations system “could alter the consumer credit database using the information contained in the Dispute Training Guide,” thus compromising the database. *Id.* The court “decline[d] to grant a protective order because of the remote *possibility* that someone *could* hack into the database and alter information, *possibly* using the information gleaned from the Dispute Training Guide,” reasoning that “[o]nce the hackers gain access, the integrity and security of [the defendant’s] system is already compromised.” *Id.* at \*3. Thus, the defendant attempted to justify sealing documents based on what a hacker could do after a hacker already had gained access. Here, in contrast, OneAmerica argues that a seal is appropriate in order to prevent a hacker from gaining access in the first place. Further, *Zahrán* was decided in 2002, more than thirteen years ago, and before the recent data breaches that occurred at Target, Anthem, and even the government. While there was a risk of data breaches then, the risk is of an even greater concern now. And, as Plaintiff argues, the risk of exposure includes a risk to the confidential personal and financial information of hundreds of thousands of its customers, including personally identifiable information such as social security numbers and account numbers.

TSNA also challenges OneAmerica’s attempt to seal information already in the public domain. There is less justification for protecting information that is already public. *See Kingery v. Quicken Loans, Inc.*, No. 2:12-CV-01353, 2014 WL 1794863, at \*4-5 (S.D.W. Va. May 6, 2014) (stating the need was not compelling). Here, however, the Court is persuaded by the assertion that the risk would be heightened because information a

hacker would otherwise have to spend time and effort to obtain is “provide[d] in a single source information.” As OneAmerica notes, under Indiana law, a compilation can constitute a trade secret or be commercially valuable even if its individual component parts would not be. *See* Ind. Code § 24-2-3-2 (defining “trade secret” under the Indiana Uniform Trade Secret Act to include a compilation of information); *N. Elec. Co. v. Torma*, 819 N.E.2d 417, 426-29 (Ind. Ct. App. 2004) (concluding that compilation of data, some of which was already in the public domain, was entitled to trade secret protection). While some information that Plaintiff seeks to protect may be public, for example, the location of its regional offices, it does not appear that information about where OneAmerica’s data centers and servers are located is also public. Further, it is the compilation of information about OneAmerica’s IT systems that OneAmerica seeks to protect.

Moreover, the Court agrees that at this stage of the litigation it is unclear that the information in the RFP and MITSA sought to be protected will be at issue in this action. Thus, the public interest in disclosure of the information relating to OneAmerica’s IT systems is weak. *See, e.g., In re Google Inc. Gmail Litig.*, 2013 WL 5366963, at \*3 (noting that the public interest in the disclosure of the information is not strong where the material “is unlikely to be critical to the substantive issue of liability”). If identification of the software, applications, hardware, vendors, regional locations, and IT policies and procedures becomes critical to the substantive issues in this case, the Court may reweigh OneAmerica’s interest in privacy and the public’s interest in transparency.

Plaintiff asks the Court to seal all of Schedule Y to the MITSA regarding OneAmerica's IT operations, policies, and procedures. It argues that the section of the MITSA reporting such information reveals its "highly confidential information," including specific passwords, system commands, and recovery processes. [*Pl.'s Br. Supp.*, doc. 42 at 13.] TSNA does not object to redacting specific passwords, system commands, and recovery processes within Schedule Y. The Court would agree that the portions of Plaintiff's IT operations, policies, and procedures should be maintained under seal. However, Schedule Y has not been filed with the Court and thus there is nothing to seal and no way to verify the contents of Schedule Y. Although the record suggests that the MITSA has Schedules identified as Schedule A through Schedule BB, the documents filed with the Court only contain schedules up to Schedule I. [*See* doc. 7-1 at 13; docs. 7-1 through 7-6.] It seems that perhaps the entire state court record has not been filed with this Court. The parties should verify that the entire record has been filed, and if not, then they should take steps to remedy any omission.

Lastly, TSNA contends that Plaintiff seeks to conceal information about OneAmerica's wrongful conduct rather than seeking to seal actual trade secret or confidential business information. The Court's review of the allegations of the *Counter-Complaint* and *Answer to the Counter-Complaint* that Plaintiff seeks to seal suggests that this may be accurate. Defendants point to one example: "while OneAmerica claims this Court should redact portions of paragraphs 8, 10, 15 and 38 of the Counter-Complaint because they specifically identify data center locations, OneAmerica then seeks to redact

information well beyond the identity of the locations.”<sup>1</sup> [TSNA’s Resp. Br., doc. 46 at 10.] The Court’s review of the unredacted *Answer to Counter-Complaint* [doc. 33] as compared to the redaction thereto [doc. 35] confirms this to be true. It seems that OneAmerica may have been overzealous in redacting information from its *Answer to the Counter-Complaint*, redacting more information than it indicates that it seeks to protect.

The same criticism can be made with respect to the other paragraphs of the *Counter-Complaint* and *Answer* (docs. 19 and 33) that OneAmerica seeks to protect. Plaintiff asserts that it seeks to protect the locations of its data centers and the identities of some of its applications, which the Court agrees should be protected, but OneAmerica’s redaction goes well beyond those pieces of information.

OneAmerica asserts that it also seeks to protect “potential vulnerabilities” in its applications, servers, and data centers. But this appears to be an effort to protect the allegations of its alleged wrongful conduct. Thus, no information shall be redacted from paragraphs 27 and 28, and only the name of the city shall be redacted from paragraph 37.

In addition, OneAmerica may redact the following information from the corresponding paragraphs *OneAmerica’s Answer to the Counter-Complaint*: from paragraph 10, line 3, the words after “network” through the end of the first sentence; and from paragraph 36, the names of the two cities and one state.

---

<sup>1</sup> Paragraph 37 of the *Counter-Complaint* also mentions the location of a data center, and it was redacted in document 35.

B. *TSNA's Motion to Seal*

Turning to TSNA's motion, OneAmerica filed a response in partial support of TSNA's motion to seal. [Doc. 66.] The response states that TSNA's *Motion to Bifurcate* does not contain any specific information about OneAmerica's IT systems, and thus, OneAmerica does not seek to seal that motion. A proposed redacted version of the *Billing Agreement* was submitted with the response. [See doc. 66-1.] OneAmerica argues that information that could put OneAmerica's and its customers' information at risk should not be exposed "particularly where that information is not central to the issues that have been briefed." [Pl. *OneAmerica Finan. Partners, Inc.'s Br. Partial Support TSNA's Mot. Seal*, doc. 66 at 2.] TSNA's *Motion to Bifurcate* concerns Section 1.1 of the *Billing Agreement*. OneAmerica asserts that the specific IT software and assets identified later in the *Agreement* are not at issue, and the parties' briefing has not cited any sections or schedules that reference them. Therefore, it seems that redaction in lieu of filing under seal in accordance with Local Rule 5-11(c) is appropriate. See S.D. Ind. L.R. 5-11(c)(2) ("When any of the confidential information in a document is irrelevant or immaterial to resolution of the matter at issue, the filing party may redact, by blacking out, the confidential information in lieu of filing under seal.") The parties and the Court should refer to the redacted copy of the *Billing Agreement* that is attached to *Plaintiff OneAmerica Financial Partners, Inc.'s Brief in Partial Support of TSNA's Motion to Seal* [see doc. 66-1.] However, the unredacted copy of the *Billing Agreement*, which is attached to *TSNA's Motion to Bifurcate and for Speedy Trial on Count III of Its Counterclaim*, shall be maintained under seal.

*Conclusion*

For the foregoing reasons, the Court **GRANTS IN PART AND DENIES IN PART** *Plaintiff's Motion to Maintain Certain Portions of Documents under Seal* [doc. 41]:

- (1) The sealed documents that are part of Electronic Filing Nos. 6 and 7 in this case [*see* docs. 6-1 through 6-4 and 7-1 through 7-6] **shall be maintained under seal**;
- (2) *Exhibit A to TSNA's Counterclaims, Excerpt from TSNA Application Collection Worksheets* [doc. 19-1] **shall be maintained under seal**;
- (3) Electronic Filing Nos. 19 and 33 **shall be maintained under seal**; and
- (4) Within 14 days of this date, the parties shall file new redacted versions of the *Counter-Complaint* [doc. 19] and *Answer to the Counter-Complaint* [doc. 33], respectively, redacting the following:
  - ¶ 8, in the third line, the six words between "in" and "and," which identify the location of one of the data centers;
  - ¶ 10, the words following "primarily housed" through the end of the sentence;
  - ¶ 15, the entire parenthetical at the end of the sentence;
  - ¶ 26, the three names of the applications contained in the parenthetical in line 3 and the name of the city in line 5;
  - ¶ 34, the name of the city and state in line 6;
  - ¶ 36(B), the name of the city in line 1;
  - ¶ 36(C), the names of the two cities and one state;
  - ¶ 37, the name of the city in the last line;
  - ¶ 38, the city and state identified on the second line;

¶ 54, the identities of the three applications at the end of the sentence; and  
*Exhibit A* to the *Counter-Complaint*.

No information shall be redacted from ¶¶ 27, 28, and 36(A) and (D); and

The following shall be redacted from corresponding paragraphs of the *Answer to Counter-Complaint*:

¶ 10, line 3, the words after “network” through the end of the sentence; and

¶ 36, the names of the two cities and one state.

The Court **GRANTS IN PART AND DENIES IN PART** *TSNA’s Motion to Seal Its Motion to Bifurcate and for Speedy Trial on Count III of Its Counterclaim* [doc. 56]. The unredacted copy of the *Billing Agreement* [doc. 55-1] **shall be maintained under seal** and OneAmerica’s proposed redacted *Billing Agreement* [doc. 66-1] shall be substituted for the unredacted version in the public record. The *Motion to Bifurcate* [doc. 55] shall be unsealed in 14 days.

SO ORDERED: 03/09/2016



Denise K. LaRue  
United States Magistrate Judge  
Southern District of Indiana

Electronic Distribution to All Counsel of Record