BEFORE THE UNITED STATES JUDICIAL PANEL ON MULTIDISTRICT LITIGATION

IN RE BLACKBAUD, INC., PRIVACY AND DATA BREACH LITIGATION	))	**MDL NO.:**

PLAINTIFF WILLIAM ALLEN'S BRIEF IN SUPPORT OF HIS MOTION FOR TRANSFER OF ACTIONS PURSUANT TO 28 U.S.C. § 1407, TO THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF SOUTH CAROLINA FOR COORDINATED OR CONSOLIDATED PRETRIAL PROCEEDINGS

Pursuant to 28 U.S.C. § 1407 and Rule 6.2 of the Rules of Procedure of the Judicial Panel on Multidistrict Litigation, Plaintiff William Allen[1] ("Movant") respectfully submits this brief in support of his Motion for Transfer of Actions Pursuant to 28 U.S.C. § 1407 to the United States District Court for the District of South Carolina for Coordinated or Consolidated Pretrial Proceedings.

Movant seeks transfer and assignment of all pending actions against Blackbaud, Inc. ("Blackbaud" or "Defendant") related to the recent data breach identified in several cases filed nationwide and as listed in the Schedule of Actions ("the Actions"), as well as any subsequently filed actions involving similar facts or claims. There are presently no fewer than eight substantially similar Actions, filed by plaintiffs on behalf of proposed nationwide and statewide classes in four different federal district courts across the country alleging similar wrongful conduct by Blackbaud. And given the breadth and severity of the issues involved, there are likely to be more. Movant Plaintiff in the first filed case in the United States District Court in the District of South Carolina, which is also the location of Blackbaud's headquarters.

[1] Movant is the named Plaintiff in the first filed in this matter in the United States District Court, *Allen, et al. v. Blackbaud, Inc.*, 2:20-cv-2930-RMG (D.S.C.).

All Actions involve common questions of law and fact that arise from the Blackbaud ransomware attack and data breach ("Data Breach") of several schools, healthcare institutions, non-profit companies, and other organizations whose data was housed, managed, maintained, stored and secured by Blackbaud. The current Actions seek redress on behalf of individuals whose Personal Identifying Information ("PII") and/or Protected Health Information (PHI) (collectively "Private Information" or "PI") was accessed and exposed because of Blackbaud's failure to reasonably and properly secure it. Upon information and belief, the Data Breach involved the Private Information of millions of individuals across the United States.

Accordingly, Movant seeks the consolidation and transfer of the Actions to the District of South Carolina, where Blackbaud is headquartered, the first two filed Actions are venued, the majority of witnesses are located, and substantial acts in furtherance of Blackbaud's alleged improper conduct occurred. All of the Actions filed against Blackbaud contain common allegations and common questions of fact. Moreover, because of the widespread nature of Blackbaud's breach and the likely impact to individuals in all 50 states and internationally, additional cases are virtually certain to be filed in the future.

I. BACKGROUND

Incorporated in 1982,[2] Blackbaud, based in South Carolina, describes itself as "the world's leading cloud software company powering social good." This includes providing its clients with "cloud software, services, expertise, and data intelligence…" Essentially, Blackbaud is in the business of selling millions of dollars in data security platforms to entities, in order for those entities to safely and securely store Private Information from donors, patients, students and others.

[2] Blackbaud 2019 Annual Report at 3 (Feb. 20, 2020), *available at* https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417.

Blackbaud is a publicly traded company with clients that include "nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them." (collectively Blackbaud's "Clients").[3] In 2019, Blackbaud reported that it had "45,000 customers located in over 100 countries."[4] In the ordinary course of doing business with Blackbaud's Clients, individual customers, donors, patients, and other individuals (collectively "Users") are regularly required to provide Defendant's Clients with sensitive, personal and private information that is then stored, maintained, and secured by Defendant. This information includes or may include customers' and donors' names, spouses' names, addresses, dates of birth, contact information, and other information that can be used to discover someone's assets, wealth, income, and identity.

In its 2019 Annual Report to investors, Blackbaud expressly acknowledged that its business of protecting the Private Information of its Users is of the utmost importance and the core of its business:

> ***If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.***
>
> Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal control measures, and physical security procedures we employ to safeguard our systems, **we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.** [Emphasis Added].
>
> Like many major businesses, we are, from time to time, a target of cyber-attacks and phishing schemes, and we expect these threats to continue. Because of the numerous and evolving cybersecurity threats, including advanced and persistent cyber-attacks, phishing and social engineering schemes, used to obtain

[3] About Blackbaud, https://www.blackbaud.com/company (last visited Aug. 12, 2020).
[4] Blackbaud Annual Report, *supra* n.3.

> unauthorized access, disable or degrade systems have become increasingly more complex and sophisticated **and may be difficult to detect for periods of time, we may not anticipate these acts or respond adequately or timely**... [Emphasis Added]…
>
> Further, the existence of vulnerabilities, even if they do not result in a security breach, may harm client confidence and require substantial resources to address, and we may not be able to discover or remedy such security vulnerabilities before they are exploited, which may harm our business, reputation and future financial results. [5]

Accordingly, Blackbaud maintained its Users' Private Information, including that of Plaintiff and putative Class Members, on what it purported to be an exceptionally secure shared network(s) and/or server(s) and utilizing appropriate security software. Despite its own awareness of steady increases of cyberattacks on Blackbaud's Clients, like healthcare institutions, schools, and other facilities over the course of recent years, Blackbaud failed to maintain adequate security of Plaintiff and putative Class Members' data, to protect against hackers and cyberattacks.

Consequently, between February and May of 2020, data thieves were able to access Blackbaud's system in an attempt to "disrupt the business by locking companies out of their own data and servers."[6] According to Defendant's statements:

> After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly… The subset of customers who were part of this incident have

[5] Blackbaud Annual Report, *supra* n.3.
[6] Blackbaud Cybersecurity Incident, https://www.blackbaud.com/securityincident (last accessed Sept. 15, 2020).

> been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.[7]

Although Blackbaud claims that social security numbers, credit card information, or bank account information was not accessed, the Client notices advise individual Users whose Private Information was accessed to, *inter alia*, "be on alert for any suspicious activity or attempts at identity theft…" *See* Exhibit A to *Allen* Complaint. Other notices from Blackbaud's Clients acknowledge that the data collected may include Social Security Numbers, copies of checks, and PHI. *See* Exhibits A and B to the *Estes* Complaint.

We now know that hundreds of Blackbaud's Clients were impacted by the attack, including numerous hospitals, schools, and museums, as well as some of the largest non-profit organizations in the United States like the YMCA, Boy Scouts of America, Planned Parenthood, the American Red Cross, the ACLU, and numerous others. As of September 11, 2020, Inova Health System alone reported that the Blackbaud Data Breach affected the Private Information of more than one million of its patients, donors, and prospective donors.[8]

As reported by the HIPAA Journal on September 11, 2020, ***at least three million individuals whose data was given to healthcare systems and entities were affected by this Data Breach***.[9] Specifically, as reported by the *HIPAA Journal*, "[t]he list below is not comprehensive but includes entities that are known to have been affected by the breach, together with the number of individuals potentially affected, where known."[10]

Breached Entity	**Individuals Affected**

[7] *Id.*
[8] *Inova Health System Says 1.05 Million Individuals Impacted by Blackbaud Ransomware Attack*, HIPAA Journal (Sept. 11, 2020), https://www.hipaajournal.com/inova-health-system-says-1-05-million-individuals-impacted-by-blackbaud-ransomware-attack.
[9] *Id.*
[10] *Id.*

Inova Health System	1,045,270
Northern Light Health	657,392
Saint Luke's Foundation	360,212
MultiCare Health System	179,189
University of Kentucky HealthCare	163,000
University of Florida Health	135,959
The Guthrie Clinic	92,064
Main Line Health	60,595
Aveanna Healthcare	166,000
Northwestern Memorial HealthCare	55,593
Spectrum Health	52,711
Richard J. Caron Foundation	22,718
SCL Health	Unconfirmed
University of Detroit Mercy	Unconfirmed
Children's Hospital of Pittsburgh Foundation	Unconfirmed
Atrium Health	Unconfirmed
NorthShore University Health System	Unconfirmed
Cancer Research Institute (NYC)	Unconfirmed
Prostate Cancer Foundation.	Unconfirmed
Total:	**2,990,703**

Blackbaud has also admitted that it could have made changes to prevent this from happening. In its release to the public about the breach, Blackbaud said: "We have already

implemented changes to prevent this specific issue from happening again."[11] Unfortunately, Blackbaud failed to do so until after the damage was done. Likewise, Blackbaud's month long delay in reporting the Data Breach to its Clients and users exacerbated and failed to mitigate the harm and risk of exposure.

Consequently, as a result of Blackbaud's failures, eight separate class action lawsuits have been filed across the United States in the last month. More will likely follow. While the claims differ slightly (but immaterially) from Complaint to Complaint, each Action names Blackbaud as the Defendant, alleges materially identical facts, and seeks certification of nationwide and/or statewide classes comprised of individuals whose data was compromised in the ransomware attack and Data Breach. Consistent with the Panel's practice in similar litigation and to promote efficiency, Plaintiff seeks transfer of the Actions to the United States District Court for the District of South Carolina for coordinated or consolidated pretrial proceedings. All of the Actions filed against Blackbaud contain common questions of fact. They are all based on the same "security incident" that led to the data breach. Lastly, Blackbaud's actions have received a great deal of publicity and individuals are still being notified of the breach, further increasing the likelihood of a number of tag-along cases in the near future.

II. LEGAL STANDARD

Transfer is appropriate when actions pending in different judicial districts involve similar questions of fact such that coordinating or consolidating pretrial proceedings would "promote the just and efficient conduct of such actions." 28 U.S.C. § 1407. In relevant part, Section 1407 provides as follows:

> When civil actions involving one or more common questions of fact are pending in different districts, such actions may be transferred to any district for coordinated or consolidated pretrial proceedings. Such transfers shall be made by

[11] Blackbaud Cybersecurity Incident, *supra* n.7.

> the judicial panel on multidistrict litigation authorized by this section upon its determination that transfers for such proceedings will be for the convenience of parties and witnesses and will promote the just and efficient conduct of such actions.

Id. *See also In re Nifedipine*, 266 F. Supp. 2d 1382, 1382 (J.P.M.L. 2003).

III. ARGUMENT

The Actions, and the many tag-along actions that will follow, are appropriate for Section 1407 transfer because they involve common factual and legal issues and transfer will benefit the parties, witnesses, and courts. Further, given Blackbaud's location in the District of South Carolina and the fact that many key witnesses will be located in that jurisdiction, transfer to that district is the most appropriate.

A. Transfer Is Appropriate Under 28 U.S.C § 1407.

"The purpose of § 1407. . . is to eliminate the potential for conflicting contemporaneous pretrial rulings by coordinate district and appellate courts in multidistrict related civil actions." *In re Plumbing Fixture Cases*, 298 F. Supp. 484, 491-92 (J.P.M.L. 1968). Centralization is meant to "eliminate duplicative discovery; prevent inconsistent pretrial rulings; and conserve the resources of the parties, their counsel, and the judiciary." *In re Ethicon Physiomesh Flexible Composite Hernia Mesh Prod. Liab. Litig.*, 254 F. Supp. 3d 1381, 1382 (J.P.M.L. 2017).

Pretrial transfer under section 1407 is appropriate and necessary here. The Actions involve nearly identical facts, the same Defendant, and similar proposed classes. The number of cases grows by the day. Absent transfer for pretrial proceedings, the Parties will incur excessive costs due to duplicative discovery from courts in South Carolina, California, Florida, and New York (at a minimum), and will face the risk of inconsistent rulings on a variety of matters.

Further, the Panel has routinely transferred similar data breach cases for coordination, including the following most recent cases: *In Re: Capital One, Consumer Data Sec. Breach*

Litig., 396 F. Supp. 3d 1364 (J.P.M.L. Oct. 2, 2019*); In Re: Marriott Int'l Inc., Data Sec. Breach Litig.*, 363 F. Supp. 3d 1372 (J.P.M.L. Feb. 6, 2019); *In Re: Uber Technologies, Inc., Data Sec. Breach Litig.*, 304 F. Supp. 3d 1351 (J.P.M.L. Apr. 4, 2018); and *In Re: Equifax, Inc., Customer Data Sec. Breach Litig.*, 289 F. Supp. 3d 1322 (J.P.M.L. Dec. 6, 2017).[12]

As these Actions share common factual allegations and causes of actions that "arise from the same data security breach, and they all allege that [Defendant] failed to put into place reasonable data protections,"[13] transfer for coordinated and consolidated pretrial proceedings is appropriate.

1. The Actions Involve Common Factual Issues.

Each of the constituent Actions will require adjudication of whether Blackbaud violated privacy law, deceptive trade practice statutes, data breach statutes, express or implied contracts, and tort laws in its manufacturing, marketing, and sale of the security platforms at issue, which failed to adequately protect the Private Information of the classes pled.

Many common questions exist in the Actions, including:

---

[12] *See also In Re: Sonic Corp. Customer Data Sec. Breach Litig.*, 276 F. Supp. 3d 1382 (J.P.M.L. Dec. 6, 2017*); In Re 21st Century Oncology Customer Data Sec. Breach Litig.*, 214 F. Supp. 3d 1357 (J.P.M.L. Oct. 6, 2016); *In re: Sprouts Farmers Market, Inc., Employee Data Sec. Breach Litig.*, 232 F.Supp.3d 1348 (J.P.M.L. Oct. 6, 2016); *In Re Cmty. Health Sys., Inc., Customer Sec. Data Breach Litig.*, 84 F. Supp. 3d 1362 (J.P.M.L. Feb. 4, 2015); *In Re: Ashley Madison Customer Data Se. Breach Litig.*, 148 F. Supp. 3d 1378 (J.P.M.L. Dec. 9, 2015); *In Re: Target Corp. Customer Data Sec.* Breach Litig., 11 F. Supp. 3d 1338, 1339 (J.P.M.L. 2014); *In Re: Zappos.com, Inc., Customer Data Sec. Breach Litig.*, 867 F. Supp. 2d 1357, 1358 (J.P.M.L. 2012); *In Re: Schnuck Markets, Inc., Customer Data Sec. Breach Litig.*, 978 F. Supp. 2d 1379, 1382 (J.P.M.L. 2013); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 870 F. Supp. 2d 1380, 1381 (J.P.M.L. 2012); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 802 F. Supp. 2d 1370, 1371 (J.P.M.L. 2011); *In re RBS Worldpay, Inc., Customer Data Sec. Breach Litig.*, 626 F. Supp. 2d 1322, 1323 (J.P.M.L. 2009); *In re: Heartland Payment Sys., Inc.*, 626 F. Supp. 2d 1336, 1337 (J.P.M.L. 2009); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 559 F. Supp. 2d 1405, 1406 (J.P.M.L. 2008); *In re: Lending Tree, LLC, Customer Data Sec. Breach Litig.*, 581 F. Supp. 2d 1367, 1368 (J.P.M.L. 2008); *In Re: Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, 588 F. Supp. 2d 1368, 1369 (J.P.M.L. 2008); *In re TJX Cos., Inc., Customer Data Sec. Breach Litig.*, 493 F. Supp. 2d 1382, 1383 (J.P.M.L. 2007); *In re Dep't of Veterans Affairs (VA) Data Theft Litig.*, 461 F. Supp. 2d1367, 1369 (J.P.M.L. 2006).

[13] *In Re: Capital One, Consumer Data Sec. Breach Litig.*, 396 F. Supp. 3d 1364 (J.P.M.L. 2019).

- Whether Blackbaud failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- Whether Blackbaud's data security systems prior to and during the Data Breach complied with applicable data privacy and security laws and regulations;

- Whether Blackbaud's data security systems prior to and during the Data Breach were consistent with industry standards;

- Whether Blackbaud owed a duty to Class Members to safeguard their Private Information;

- Whether Blackbaud breached its duty to Class Members to safeguard their Private Information;

- Whether computer hackers obtained and used or sold Class Members' Private Information in the Data Breach;

- What Private Information was accessed;

- Whether Blackbaud knew or should have known that its data security systems and monitoring processes were deficient;

- Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

- Whether Blackbaud's conduct was negligent;

- Whether Blackbaud's conduct was *per se* negligent;

- Whether Blackbaud's acts, inactions, and practices complained of herein amount to violation of privacy law including acts of intrusion upon seclusion;

- Whether Blackbaud failed to timely provide notice of the Data Breach;

- Whether Blackbaud breached its duty or violated the law in its notification of those impacted;

- Whether Plaintiff and putative Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief; and

- Whether class certification is appropriate.

The near identity of claims means that any court tasked with resolving one of these lawsuits would face the same basic legal and factual issues. Adjudicating these and other common issues in a single transferee district will benefit the Parties and witnesses, as well as promote judicial efficiency by allowing a single court to coordinate the pretrial proceedings governing claims with these issues.

2. Transfer Will Serve The Convenience Of The Parties And Witnesses And Will Promote The Just And Efficient Conduct Of The Actions.

According to the Manual for Complex Litigation, the following four factors govern whether transfer will facilitate the convenience of the parties and promote the just and efficient conduct of the transferred cases:

1. The elimination of duplicative discovery;
2. The avoidance of conflicting rules and schedules;
3. The reduction of litigation cost; and
4. The conservation of the time and effort of the parties, attorneys, witnesses, and courts.

Manual for Complex Litigation (Fourth), § 20.131, at 219.

With eight cases in three different Districts—and with those numbers likely to materially increase—the size of this litigation weighs in favor of transfer. Indeed, without transfer, this litigation, which addresses serious security flaws contained within the Blackbaud platforms intended to secure PI data collected by numerous hospitals, schools, non-profits and other organizations throughout the United States and the world, needless and unnecessary expense of overlapping discovery (including expert discovery) and judicial inefficiency would result.

Further, different federal courts would make duplicative rulings on the same issues, which could result in contradictory findings on significant pretrial disputes. Litigation of this scope and importance should not be with such inconsistencies and inefficiencies.

Consolidation will also maximize efficiencies and expedite the resolution of the Actions because they are all at their procedural infancy. *See In re Johnson & Johnson Talcum Powder Prod. Mktg., Sales Practices & Prod. Liab. Litig*., 220 F. Supp. 3d 1356, 1358 (U.S. Jud. Pan. Mult. Lit. 2016) (granting consolidation after finding the actions were not too procedurally disparate to benefit from centralization where nearly all were filed within the past six months); *In re Ambulatory Pain Pump-Chondrolysis Prods. Liab. Litig*., 709 F. Supp. 2d 1375 (J.P.M.L. 2010) (denying centralization of 102 actions because panel was "unconvinced that centralization would serve the convenience of the parties" in actions at "widely varying procedural stages.").

a. Transfer Will Eliminate Duplicative Discovery.

Because each of the Actions is based upon the same facts, Plaintiffs in each of the Actions are, in turn, inevitably seeking overlapping discovery. *See In re Auto Body Shop*, 2014 WL 3908000, at *1-2 (J.P.M.L. 2014) (noting that transfer was appropriate to eliminate duplicative discovery when the actions shared a common factual core). The Actions are also likely to involve complex technical issues regarding software coding, security software vulnerabilities, remote server and other architecture, which will involve substantial expert discovery and *Daubert* briefing and hearings. These facts alone militates in favor of transfer. *See, e.g., In re Natrol, Inc. Glucosamine/Chondroitin*, 2014 WL 2616783, at *1 (J.P.M.L. 2014). Similarly, Plaintiffs in each of the Actions are likely to seek to depose many of the same Blackbaud witnesses, including software engineers, sales and marketing employees, as well as others. The overlapping facts, factual issues, and location of fact witnesses again favors

centralization in South Carolina. *See, e.g.*, *In re Auto Body Shop*, 2014 WL 3908000, at *1 (transfer to a single judge was beneficial because he or she could "structure pretrial proceedings to accommodate all parties' legitimate discovery needs while ensuring that common witnesses are not subjected to duplicative discovery demands"); *In re Enfamil Lipil*, 764 F. Supp. 2d 1356, 1357 (J.P.M.L. 2011) ("Centralizing the actions will allow for the efficient resolution of common issues and prevent unnecessary or duplicative pretrial burdens from being placed on the common parties and witnesses.").

Given the similarity of the Actions and the potential for duplicative discovery, transfer would inevitably conserve the Parties' resources. *See, e.g., In re Air Crash at Dallas/Fort Worth Airport*, 623 F. Supp. 634, 635 (J.P.M.L. 1985). It would also conserve the courts' resources, as it would assign responsibility for overseeing a pretrial plan to one judge as opposed to many different federal judges. *See, e.g.*, *In re PineBlackbaud*, 342 F. Supp. 2d 1348, 1349 (J.P.M.L. 2004).

b. Transfer will Avoid Conflicting Rules and Schedules.

The Panel considers the possibility of inconsistent rulings on pretrial issues because of the possible *res judicata* or collateral estoppel effects on other cases. *See In re Enron Securities Derivative & ERISA Litig*., 196 F. Supp. 2d 1375, 1376 (J.P.M.L. 2002) (granting a transfer in part to prevent inconsistent pretrial rulings, particularly with respect to questions of class certification).

Pretrial procedures will necessarily involve motions to dismiss, discovery motions, *Daubert* motions, and class certification motions. Conflicting rulings on these motions will cause unnecessary confusion and duplicative effort. Further, although only three district courts have cases now, given the sheer number of Users affected by the Data Breach in all parts of the

country, there will undoubtedly be many more materially similar cases filed across the United States.

Section 1407 transfer is the most efficient way to ensure that pretrial processes across all of these cases are uniformly litigated and adjudicated, thereby avoiding the situation where multiple courts reach contrary conclusions and potentially subject litigants to conflicting responsibilities and obligations.

c. Transfer will Reduce Litigation Costs and conserve the time and effort of the parties, attorneys, witnesses, and courts.

Each of the Actions, and the tag-along actions to follow, will benefit from having a single transferee judge address and adjudicate issues related to discovery and pretrial motion practice. If the Actions are not transferred and consolidated, courts and lawyers will be briefing the same issues in several different district courts, across several circuits, with conflicting laws, witnesses will be called to depositions in numerous cases, and third-parties will be called to produce documents and witnesses in several different cases.

B. <u>The District of South Carolina Is the Most Appropriate Transferee Forum.</u>

The Panel can consider the nexus between the transferee forum and the parties to the litigation when resolving transfer requests under 28 U.S.C. § 1407. A significant "nexus" exists when a party who is common to all actions (*e.g.*, the sole defendant) is headquartered or has facilities that are located within the transferee court's jurisdiction, such that relevant witnesses and documentary evidence common to all the actions are likely to be found there. *See, e.g., In re Equifax, Inc.*, MDL No. 2800, 2017 WL 6031680, at *2 (J.P.M.L. Dec. 6, 2017) (transferring actions to the district where the main defendant is headquartered as "relevant documents and witnesses thus likely will be found there."); *In re Wells Fargo Auto Ins. Mktg. & Sales Practices Litig.*, MDL No. 2797, 2017 WL 4737285, at *1 (J.P.M.L. Oct. 19, 2017) ("it is alleged that key

entities and individuals with direct responsibility for the alleged conduct in this litigation are located in [the transferee] district and, therefore, relevant documents and witnesses may be located there."); *In re Google Inc. St. View Elec. Commc'ns Litig*., 733 F. Supp. 2d 1381, 1382 (J.P.M.L. 2010) (transferring cases to Northern District of California where "[t]he sole defendant, Google, is headquartered there, and most relevant documents and witnesses are likely located there."); *In re Sears, Roebuck & Co. Tools Mktg. & Sales Practices Litig*., 381 F. Supp. 2d 1383, 1384 (J.P.M.L. 2005) ("relevant discovery will likely be found within this district, because Sears's corporate headquarters and many of its documents and witnesses are located there"); *St. Jude Med., Inc., Silzone Heart Valves Prod. Liab. Litig*., MDL No. 1396, 2001 WL 36292052, at *2 (J.P.M.L. Apr. 18, 2001) (transferring litigation to district because "as the situs of the headquarters of the sole defendant in all actions, the district is likely to be a substantial source of witnesses and documents subject to discovery").

The District of South Carolina is the most appropriate transferee district for this litigation. Blackbaud has been headquartered in South Carolina since 2000, and specifically Daniel Island, Charleston County, South Carolina.[14] The Panel regularly transfers cases to the district where the defendant is located, and this litigation should not be an exception. *See, e.g.*, *In re Equifax*, 2017 WL 6031680, at *2; *In re: Toyota Motor Corp. Hybrid Brake Mktg., Sales Practices, & Prod. Liab. Litig*., 732 F. Supp. 2d 1375, 1377 (J.P.M.L. 2010). Blackbaud's software engineers, sales and marketing departments are located at its South Carolina headquarters and those departments will be focal points for discovery in this litigation.[15] This makes South Carolina the ideal district for transfer. *In Re: Allura Fiber Cement Siding, Prod. Liab. Litig.*, 366 F. Supp. 3d 1365 (April

[14] Nicole McGougan, *Blackbaud Inaugurates New World Headquarters in South Carolina*, Blackbaud Newsroom (Jun. 12, 2018), https://www.blackbaud.com/newsroom/article/2018/06/12/blackbaud-inaugurates-new-world-headquarters-in-south-carolina.

[15] Available Jobs, Blackbaud, https://blackbaud.wd1.myworkdayjobs.com/ExternalCareers/0/refreshFacet/318c8bb6f553100021d223d9780d30be (last visited September 12, 2020).

2, 2019) ("We conclude that the District of South Carolina is an appropriate transferee forum. One action on the motion is pending there, and the district is conveniently located for a number of parties and potential witnesses in the southeastern region of the country.").

Finally, the District of South Carolina (Charleston Division) already has the first two filed cases and many judges with exceptional records in handling complex litigation and MDLs. *See, e.g., In Re: Bausch & Lomb, Inc. Contact Lens Solutions Products Liability Litigation*, 444 F.Supp. 2d 1336 (J.P.M.L. 2006)(Hon. David C. Norton); *In Re: Lipitor Mktg., Sales Practices, and Prod. Liab. Litig. (No. II)*,997 F. Supp. 2d 1354 (J.P.M.L. 2014)(Hon. Richard M. Gergel); *In Re: MI Windows and Doors, Inc., Prod. Liab. Litig.*, 857 F. Supp. 2d 1374 (J.P.M.L. 2012)(Hon. David C. Norton)(noting the Honorable David C. Norton is an "experienced transferee judge"); *In Re: Pella Corp. Architect and Designer Windows Mktg., Sales Practices and Prod. Liab. Litig.*, 996 F. Supp. 2d 1380 (J.P.M.L. 2014)(Hon. David C. Norton); *In Re: Allura Fiber Cement Siding Prod, Liab. Litig.*, 366 F. Supp. 3d 1365 (J.P.M.L. 2019)(Hon. David C. Norton); *In Re: TD Bank, N.A., Debit Card Overdraft Fee Litig.*, 96 F. Supp. 3d 1378 (J.P.M.L. 2015); *In Re: Aqueous Film-Forming Foams Prod. Liab. Litig.*, 357 F. Supp. 3d 1397 (J.P.M.L. 2018). Notably, the District of South Carolina currently has just three MDLs to manage;[16] and one of those three, the *Allura* MDL before Judge Norton, will likely be resolved within the next six months.[17]

---

[16] MDL Statistics Report—Distribution of Pending MDL Dockets by District, https://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_District-August-17-2020.pdf (last visited Sept. 15, 2020).

[17] Whitfield Bryson, LLP has lawyers serving as Lead Counsel and on Plaintiffs' Steering Committee in the *Allura* litigation and has personal knowledge about the progress of that litigation.

Transfer of the pending Actions to the District of South Carolina will serve the convenience of the parties and witnesses and promote the just and efficient conduct of this litigation.

IV. CONCLUSION

For the above-stated reasons, Movant respectfully requests that the Panel transfer the Actions set forth on the attached Schedule and all subsequently filed tag-along cases for coordinated or consolidated pretrial proceedings in the United States District Court for the District of South Carolina.

September 18, 2020

Respectfully submitted,

/s/ *Harper Todd Segui*
Harper Todd Segui
WHITFIELD BRYSON LLP
217 Lucas Street, Suite G
Mount Pleasant, SC 29464
Tel: (919) 600-5000
Fax: (919) 600-5035
Email: harper@whitfieldbryson.com

Matthew E. Lee
Erin J. Ruben
WHITFIELD BRYSON LLP
900 W. Morgan Street
Raleigh, NC 27603
T: 919-600-5000
Fax: 919-600-5035
Email: matt@whitfieldbryson.com
erin@whitfieldbryson.com

Attorneys for Plaintiff William Allen