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

KATHRYN MORTENSEN, individually and on behalf of all others similarly situated, Plaintiff, v. BLACKBAUD, INC., a South Carolina Resident, Defendant.	Case No.: 2:20-cv-4042-RMG **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kathryn Mortensen ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, brings this Class Action Complaint and alleges the following against Blackbaud, Inc., ("Blackbaud" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Blackbaud for Blackbaud's failure to properly secure and safeguard protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information, including without limitation names, dates of birth, phone numbers, addresses, health insurance information, and medical treatment information (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain that PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, orders requiring Blackbaud to fully and accurately disclose the nature of the information that has been

compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, and to provide for the lifetimes of Plaintiff and Class Members identity theft protective services as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of Blackbaud as described herein.

2. Blackbaud is a publicly traded company that provides its customers with cloud-based software, services, expertise, and data intelligence. Blackbaud has "millions of users" located in over 100 countries around the world.[1]

3. Blackbaud's customers include nonprofits, foundations, corporations, educational institutions, healthcare institutions, and the individual change agents who support them.[2]

4. In the course of doing business with Blackbaud's customers, individuals such as Plaintiff are regularly required to provide either Blackbaud's customers or Blackbaud directly with their PII. That PII is then stored on Blackbaud's cloud.

5. On or about September 9, 2020, Nuvance Health ("Nuvance"), a healthcare facility and customer of Blackbaud, notified its patients, including Plaintiff, that their PII, which Nuvance was storing on Blackbaud's cloud, had been illegally exposed to unauthorized third parties between February 7, 2020 and May 20, 2020. (the "Data Breach"). An exemplar of the Notification of Data Security Incident letter from Nuvance dated September 9, 2020 (the "Notice Letter") that was sent to Plaintiff is attached hereto as Exhibit "A."

6. Since the announcement of the Data Breach, other healthcare facilities have issued similar notices, indicating that their patients also had PII compromised in the wide-reaching Data Breach. The Data Breach compromised the PII of 314,829 patients at Nuvance

[1] https://www.blackbaud.com/company (Last Accessed Oct. 28, 2020).
[2] *Id.*

alone, according to Nuvance's notice to the U.S. Secretary of Health and Human Services at the Office for Civil Rights.[3]

7. Blackbaud has indicated to health care facilities such as Nuvance that during the period of the Data Breach, a third party was not only able to view Plaintiff and Class Members' PII, but was also able to subsequently remove that data from Blackbaud's cloud system.

8. As a result of Blackbaud's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Blackbaud's failures.

9. Plaintiff, on behalf of herself and all others similarly situated, alleges claims for for negligence, negligence *per se*, breach of implied contract, unjust enrichment, declaratory judgment, breach of confidence, violation of South Carolina's Data Breach Security Act, S.C. Code Ann. §§ 39-1-90, and invasion of privacy. Plaintiff seeks to compel Blackbaud to adopt reasonably sufficient practices to safeguard PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

10. Plaintiff Kathryn Mortensen is a citizen and resident of Wilton, Connecticut. At all times relevant to this Complaint, Ms. Mortensen was a patient of Nuvance, whose PII was disclosed without authorization to an unknown third party as a result of the Blackbaud Data

[3] Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 1, 2020).

Breach.

11. On or about September 9, 2020, Plaintiff received a letter from Nuvance stating that Blackbaud, one of Nuvance's vendors, experienced a data security incident. Plaintiff was informed that Nuvance was one of the affected healthcare institutions. Nuvance advised Plaintiff that as a result of the Data Breach, unauthorized third parties were able to view and acquire data from Blackbaud containing her PII.

12. Since the announcement of the Data Breach, Plaintiff has been required to spend her valuable time to monitor her various accounts in an effort to detect and prevent any misueses of her PII – time which she would not have had to expend but for the Data Breach.

13. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come.

14. Defendant Blackbaud is a corporation organized under the laws of Delaware with a principal place of business at 2000 Daniel Island Drive, Charleston, South Carolina, 29492. It is a cloud-based software company that provides services for customers located in many countries around the world.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a different state from Defendant.

16. This Court has personal jurisdiction over Blackbaud because Blackbaud maintains its principal place of business in this District and is authorized to and does conduct substantial business in this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, Blackbaud is based in this District, Blackbaud maintains Plaintiff's and Class Members' PII in this District, and has caused harm to Plaintiff and Class Members residing in this District.

FACTUAL BACKGROUND

A. Blackbaud's Business

18. Blackbaud markets itself as a leading cloud software company that is "driving the digital transformation of the social good community." Blackbaud claims to enable effectiveness and amplify impact "across the ecosystem of good."[4]

19. Blackbaud specifically advertises itself as the "cloud soultuion for healthcare organizations." According to Blackbaud's website, 30 out of the top 32 largest non-profit hospitals use Blackbaud's cloud services. Blackbaud boasts: "[w]ith 35 years of industry leadership, no other partner provides unmatched data intelligence and comprehensive capabilities…"[5]

20. As part of its relationship with healthcare organizations, Blackbaud routinely acquires and stores patient PII on its cloud. Healthcare organizations save money by using Blackbaud's service for collecting and storing data by not having to pay for the cost of excessive capacity or maintaining the infrastructure required of a dedicated server.

[4] https://www.blackbaud.com/company (Last Accessed Nov. 1, 2020).
[5] https://www.blackbaud.com/who-we-serve/healthcare-organizations (Last Accessed Nov. 1, 2020).

21. The primary downside of cloud computing is the increased data security risk inherent in its use.[6] Nevertheless, Blackbaud promises that it is "committed to protecting [consumer] privacy."[7]

22. Healthcare patients demand security to safeguard their PII. As a vendor storing healthcare related data, Blackbaud is required to ensure that such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

B. The Data Breach

23. On or about September 9, 2020, Nuvance transmitted a Notice Letter to Plaintiff stating that Blackbaud, one of Nuvance's outside vendors, experienced a security incident that affected, among other healthcare systems, Nuvance. The Notice Letter indicated that between February 7, 2020 and May 20, 2020, an unauthorized third party was able to gain access to Blackbaud's cloud computing platform housing Nuvance patients' PII.

24. Nuvance learned about this incident from Blackbaud on July 16, 2020. Blackbaud, however, had known about this incident since May 2020. Blackbaud's notice to its customers states, in relevant part:

> In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. 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

[6] *See, e.g.*, *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, CARNEGIE MELLON UNIVERSITY BLOG (March 5, 2018), *available at*: https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html (Last Accessed Nov. 2, 2020).

[7] https://www.blackbaud.com/company/privacy-policy/north-america (Last Accessed Nov. 5, 2020).

> subset of data from our self-hosted (private cloud) environment. 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. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted environment. The subset of customers who were part of this incident have 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.[8]

25. Upon information and belief, as late as August 29, 2020, Blackbaud represented to its customers that the unauthorized third party did not have access to credit card information, bank account information, or social security numbers. Blackbaud has since amended its statement, now affirming that "[f]urther forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields indended for bank account information, social security numbers, usernames and/or passwords."[9]

26. During the Data Breach, the unauthorized third party was not only was able to view Plaintiff and Class Members' PII, but was able to intermittently remove the data from the cloud platform throughout the three month period.

27. After learning of the Data Breach from Blackbaud, Nuvance commenced its own investigation. That investigation is ongoing, but has so far revealed that approximately 314,829 Nuvance patients alone were victims of the Data Breach.

28. Nuvance, either during its own investigation or relying on the investigation commenced by its cloud vendor, determined that the data accessed and removed by the

[8] https://www.blackbaud.com/securityincident (last visited Oct. 29, 2020).
[9] *Id.*

unauthorized third party consisted of patient health information, including names, contact information, ages, genders, dates of birth, admission dates, hospital departments visited, treating physicians, and health insurance information.

29. Nuvance attests that the Nuvance electronic medical record system was not affected by this incident, yet neither Nuvance nor Blackbaud explain how the third party gained access to information regarding Plaintiff and Class Members' heath care provider names, dates of service, and hospital departments visited.

30. Blackbaud represents that the affected backup was destroyed by the unauthorized individual and that it has no reason to believe any data was or will be misused, disseminated, or otherwise made publicly available. Blackbaud provides no details to affected Class Members as to how it knows the data was in fact deleted or that it was not distributed to others prior to deletion. Instead, Blackbaud asks Plaintiff and Class Members to rest assured on a thief's promises that such information was destroyed.

31. Blackbaud claims that it has since taken steps of reduce the risk of similar incidents occurring in the future. According to Blackbaud, it: (1) has identified the vulnerability associated with the incident and has taken actions to remediate it and (2) is accelerating its efforts to implement additional security enhancements to its products, services, and internal systems.[10] Blackbaud failed, however, to provide basic details concerning the Data Breach, including, but not limited to, why sensitive patient information was stored with a cloud computing vendor which clearly did not have adequate security systems, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or

[10] *See* Exhibit A.

otherwise protected, and whether Blackbaud has confirmation that the data has actually been deleted and not otherwise disseminated.

32. Blackbaud has offered absolutely no identity theft monitoring services to Plaintiff and Class Members. Blackbaud has left Plaintiff and Class Members scrambling to find ways to protect themselves from inevitable fraud and identity theft.

33. Plaintiff's and Class Members' PII is likely for sale to criminals on the dark web, meaning even more unauthorized persons have accessed and viewed Plaintiff's and Class Members' personal information.

C. Healthcare Information is Particularly Vulnerable to Data Breaches

34. Blackbaud, a company that prides itself on being the cloud solution for 30 of the top 32 largest nonprofit hospitals and a leading platform for healthcare organizaitons, has a responsibility for keeping the patient PII that it receives safe from harm. Blackbaud was on notice that PII, specifically when it includes health information, is a target for data breaches.

35. Blackbaud was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[11]

36. The American Medical Association ("AMA") has also warned healthcare

[11] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed Oct. 27, 2020).

companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[12]

37. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[13] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[14] That trend continues.

38. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[15] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30

---

[12] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Oct. 30, 2020).

[13] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed Oct.. 27, 2020).

[14] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed Nov. 8, 2020).

[15] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed Nov. 8, 2020).

[16] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Sept. 28, 2020).

percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[17]

39. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[18] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[19]

40. As the number of healthcare data breaches continues to rise, a commonly identified vulnerability is a misconfigured cloud server.[20]

41. Blackbaud knew, or should have known, the importance of safeguarding the patients' PII entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on patients as a result of a breach.

---

[17] *Id.*
[18] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last accessed Sept. 28, 2020).
[19] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed Sept. 28, 2020).
[20] Atlantic.Net Blog, *Data Breaches Caused by Misconfigured Servers Within a Healthcare Environment*, September 2, 2019, *available at*: https://www.atlantic.net/hipaa-data-centers/data-breaches-caused-by-misconfigured-servers-within-a-healthcare-environment/(last accessed Oct. 10, 2020).

Blackbaud failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Blackbaud Obtains, Collects, and Stores Plaintiff's and Class Members' PII

42. In the ordinary course of doing business with Blackbaud's customers, Plaintiff and Class Members are regularly required to provide either Blackbaud's customers or Blackbaud directly with sensitive, personal and private protected health information which is then collected, stored, and maintained by Blackbaud.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Blackbaud assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

44. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on Blackbaud to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

45. Blackbaud acknowledges its obligation to maintain the privacy of individual PII entrusted to it. For example, Blackbaud's Privacy Policy North America ("Privacy Policy") states as follows:

> At Blackbaud, we are committed to protecting your privacy. This Policy applies to Blackbaud's collection and use of personal data in connection with our marketing and provision of the Blackbaud Solutions, customer support and other services (collectively, the "Services"), for example if you are a customer, visit the website, interact with us at industry conferences, or work for a current or prospective customer of the Services.
>
> If you're a constituent, supporter, patient or student of one of our customers, to which we provide the Services, your data will be used in accordance with that

> customer's privacy policy. In providing the Services, Blackbaud acts as a service provider and thus, this Policy will not apply to constituents of our customers.[21]

46. With regard to securing its constituents, supporters, patients or students of one of Blackbaud's customers, Blackbaud further represents with regard to the security of personal information:

> We restrict access to personal information collected about you at our website to our employees, our affiliates' employees, those who are otherwise specified in this Policy or others who need to know that information to provide the Services to you or in the course of conducting our business operations or activities. While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons.
>
> We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company's business ethics standards and confidentiality policies. Inside Blackbaud, data is stored in password-controlled servers with limited access.[22]

47. Yet, despite Blackbaud's "commitment to protecting privacy," Blackbaud failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII.

48. Blackbaud had the resources to prevent a breach. In 2019, Blackbaud reported that it had 45,000 customers located in over 100 countries, with a total addressable market greater than $10 billion.[23]

49. Had Blackbaud remedied the deficiencies in its information storage and security

[21] https://www.blackbaud.com/company/privacy-policy/north-america (Last Accessed August 12, 2020).
[22] https://www.blackbaud.com/company/privacy-policy/north-america (Last Accessed Nov. 9, 2020).
[23] https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417 (Last Accessed Oct. 30, 2020).

systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Blackbaud would have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

E. The Value of Private Information and the Effects of Unauthorized Disclosure

50. Blackbaud was well aware that the protected health information and personally identifiable information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

51. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[24] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected health information on multiple underground Internet websites, commonly referred to as the dark web.

52. While credit card information and associated personally identifiable information can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[25]

53. Protected health information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

---

[24] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Oct. 27, 2020).

[25] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Oct. 27, 2020).

54. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[26]

55. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

56. The ramifications of Blackbaud's failure to keep its patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

57. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

58. Approximately 21% of victims do not realize their identify has been compromised

[26] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://khn.org/news/rise-of-indentity-theft/ (last visited Oct. 27, 2020).

until more than two years after it has happened. [27] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[28]

59. Breaches are particularly serious when they involve medical information. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[29] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[30] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a

[27] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed Oct. 27, 2020).
[28] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accesses Oct. 27, 2020).
[29] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://notified.idtheftcenter.org/s/resource (last accessed Oct. 27, 2020).
[30] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Oct. 27, 2020); *see also*, National Survey on Medical Identity Theft, Feb. 22, 2010, cited at p. 2.

crippling effect on individuals and detrimentally impact the economy as a whole.[31]

60. Blackbaud knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. Blackbaud failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

F. Blackbaud's Conduct Violates HIPAA

61. The HIPAA Privacy Rule applies to covered entities such as health plans, health care clearinghouses, and certain health care providers. The Privacy Rule allows covered providers and health plans, however, to disclose protected information to "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misue, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.[32]

62. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provide services to, a covered entity.[33]

63. Blackbaud acknowledges that it is acting as a business assoiate when protected health information is being stored on its cloud and it has entered into a business associate agreement with a covered entity. Blackbaud promises that it complies with the HIPAA Privacy Rule by restricting its use or disclosure of protected health information to purposes authorized by

---

[31] *Id.*
[32] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (Last Accessed Nov. 10, 2020).
[33] *Id.*

patients. Blackbaud states that it complies with HIPAA by providing patients "with a secure environment for [their] PHI and adopting strict policies and procedures governing processes that could affect [patient] PHI.[34]

64. Blackbaud acts as a business associate in its relationship with covered entites such as Nuvance.

65. Blackbaud's Data Breach resulted from a combination of insufficiencies that indicate Blackbaud failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Blackbaud's Data Breach that Blackbaud either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff's and Class Members' PII.

66. In addition, Blackbaud's Data Breach could have been prevented if Blackbaud implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII when it was no longer necessary and/or had honored its obligations.

67. The Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), the American Recovery and Reinvestment Act of 2009, and Part I – Improved Privacy Provisions and Security Provisions located at 42 U.S.C. §§ 17931 and 17934, require business associates of covered entittes to comply with HIPAA, as set forth in, but not limited to 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316, 45 C.F.R. § 164.502(e)(2), and 45 C.F.R. § 164.504(e)(2013). These sections apply to a business associate of a covered entity in

[34] https://www.blackbaud.com/files/HIPAA-and-Blackbaud-Solutions.pdf?_ga=2.186566377.1128423130.1604959231-1715947792.1604423273&_gac=1.87046634.1604959369.Cj0KCQiA7qP9BRCLARIsABDaZzi9PkFAEO7Y53YxC40pVKLUx5EIyL8LunxnLX5INqSs8Qj6n98GW1waAkSLEALw_wcB (Last Accessed Nov. 10, 2020).

the same manner that such sections apply to a covered entity.

68. Blackbaud's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Blackbaud receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

69. Because Blackbaud has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Blackbaud's approach to information security is adequate and appropriate. Blackbaud still maintains the protected health information and other PII of Plaintiff and Class Members, and without the supervision of the Court via injunctive relief, Plaintiff and Class Members' protected health information and other PII remains at risk of subsequent Data Breaches.

G. Blackbaud Failed to Comply with FTC Guidelines

70. Blackbaud was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-

making.[35]

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[36] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

73. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[37]

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. Blackbaud failed to properly implement basic data security practices. Blackbaud's

---

[35] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Oct. 27, 2020).

[36] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Oct. 27, 2020).

[37] FTC, *Start With Security*, *supra* note 16.

failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Blackbaud was at all times fully aware of its obligation to protect the PII of patients because of its position as a cloud solution for healthcare organizations. Blackbaud was also aware of the significant repercussions that would result from its failure to do so.

H. Plaintiff and Class Members Suffered Damages.

77. The ramifications of Blackbaud's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[38]

78. Blackbaud's delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Although their PII was improperly exposed as early as February 7, 2020, Nuvance was not notified of the Data Breach until July 16, 2020. Plaintiff and Class Members did not receive notice until September 9, 2020. This delayed notice deprived Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

79. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[38] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Oct. 27, 2020).

80. Despite all of the publicly available knowledge of the continued compromises of PII, Blackbaud's approach to maintaining the privacy of protected health information and other PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

81. As a result of a result of Blackbaud's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise, publication, and/or theft of their PII;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies;

j. The diminished value of Blackbaud's goods and services they received;

k. Lost opportunity and benefits of electronically filing of income tax returns;

l. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

m. The continued risk to their PII, which remains in the possession of Blackbaud and is subject to further breaches so long as Blackbaud fails to undertake appropriate measures to protect the PII in its possession; and

n. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

82. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civile Procedure.

83. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals in the United States whose protected health information was compromised in the Blackbaud Data Breach which occurred between February 7, 2020 and May 20, 2020.

84. Excluded from the Class are the officers, directors, and legal representatives of Blackbaud, and the judges and court personnel in this case and any members of their immediate families.

85. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

86. Numerosity. Fed. R. Civ. P. 23(a)(1): The Class Members are so numerous that joinder of all Members is impractical. In its report to the U.S. Department of Health and Human Services - Office for Civil Rights, Nuvance alone attested that the Data Breach affected at least

314,829 of its patients.

87. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by storing that information on computers and hard drives in the manner alleged herein, including failing to comply with industry standards;

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

h. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiff and Class Members on the other;

i. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

k. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

o. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

p. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and

q. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

88. Typicality. Fed. R. Civ. P. 23(a). Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was disclosed by Blackbaud. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Blackbaud. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

89. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Blackbaud has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible

standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Blackbaud's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Blackbaud's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

90. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation and in particular privacy class litigation, and Plaintiff intends to prosecute this action vigorously.

91. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Blackbaud. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

92. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to

afford relief to Plaintiff and the Class for the wrongs alleged because Blackbaud would necessarily gain an unconscionable advantage since Blackbaud would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

93. The litigation of the claims brought herein is manageable. Blackbaud's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

94. Unless a Class-wide injunction is issued, Blackbaud may continue in its failure to properly secure the PII of Class Members, Blackbaud may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Blackbaud may continue to act unlawfully as set forth in this Complaint.

95. Further, Blackbaud has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under the Federal Rules of Civil Procedure.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

96. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

97. Blackbaud owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Blackbaud's data security systems to ensure that Plaintiff's and Class Members' PII in Blackbaud's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its data systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data and cyber security measures consistent with industry standards.

98. Blackbaud knew that the PII belonging to Plaintiff and the Class contained personal, sensitive medical information that is valuable to identity thieves and other criminals. Blackbaud also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiff and the Class were not told about the disclosure in a timely manner.

99. Blackbaud had a common law duty to prevent foreseeable harm to those whose PII it stored on its cloud. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Blackbaud knew that it was more likely than not Plaintiff and other Class Members would be harmed.

100. Blackbaud had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to

unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Blackbaud's security protocols to ensure that Plaintiff's and Class Members' information in Blackbaud's possession was adequately secured and protected.

101. Blackbaud is morally culpable, given the prominence of data breaches in the healthcare field and it's self-proclaimed proficiency in collecting and storing health care data.

102. Blackbaud breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's PII.

103. Blackbaud breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. Blackbaud breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose in a timely fashion that Plaintiff's and Class Members' PII in Blackbaud's possession had been or was reasonably believed to have been, stolen or compromised.

104. Blackbaud's failure comply with industry and federal regulations further evidences Blackbaud's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII.

105. Blackbaud's breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Blackbaud to acknowledge and correct serious and ongoing data and cyber security problems.

106. But for Blackbaud's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Blackbaud's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

107. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Blackbaud's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII. Blackbaud knew its systems and technologies for processing and securing the PII of Plaintiff and the Class had numerous security vulnerabilities.

108. As a result of this misconduct by Blackbaud, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

109. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

110. Violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury constitute may constitute negligence *per se.*

111. Section 5 of the FTC Act prohibits ""unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Blackbaud, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Blackbaud's duty in this regard.

112. Blackbaud violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and not complying with applicable industry standards, as described in detail herein. Blackbaud's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

113. Blackbaud's violation of Section 5 of the FTC Act constitutes negligence *per se.*

114. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

116. Blackbaud's violations of HIPAA also constitute negligence *per se*.

117. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access

to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

118. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

119. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

120. As a direct and proximate result of Blackbaud's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Blackbaud's possession and is subject to further unauthorized disclosures so long as Blackbaud fails to undertake appropriate and adequate measures to protect the PII of patients and former patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Blackbaud's goods and services Plaintiff and Class Members received.

121. As a direct and proximate result of Defendant's negligence, Plaintiff and Class

Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

122. Plaintiff restates and realleges all preceding paragraphs as if fully set forth herein.

123. Plaintiff and Class Members were required to provide their PII, including names, addresses, dates of birth, medical histories, and other personal information to Blackbaud and Blackbaud's customers in exchange for Blackbaud and Blackbaud's customers' services.

124. Blackbaud solicited and invited Plaintiff and Class Members to provide their PII as part of Blackbaud's regular business practices. Plaintiff and Class Members accepted Blackbaud's offers and provided their PII to Blackbaud.

125. As part of these transactions, Blackbaud agreed to safeguard and protect the PII of Plaintiff and Class Members. Blackbaud assures the public that it complies with HIPAA standards and ensures that Plaintiff's and Class Members' protected health information and other PII remains protected.

126. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Blackbaud's data and cyber security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Blackbaud would use part of the monies paid to Blackbaud either by them directly or through Blackbaud's customers, to fund adequate and reasonable data and cyber security practices.

127. Plaintiff and Class Members would not have provided and entrusted their health related information to Blackbaud or Blackbaud's customers or would have paid less for

Blackbaud's services in the absence of the implied contract or implied terms between them and Blackbaud. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

128. Plaintiff and Class Members fully performed their obligations under the implied contracts with Blackbaud.

129. Blackbaud breached its implied contracts with Plaintiff and Class Members to protect their PII when it: (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

130. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA.

131. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

132. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

133. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

134. Blackbaud further breached the implied contracts with Plaintiff and Class

Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

135. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

136. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

137. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

138. Blackbaud further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

139. Blackbaud further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

140. Blackbaud further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

141. Blackbaud's failures to meet these promises constitute breaches of the implied contracts.

142. As a direct and proximate result of Blackbaud's breach of its implied contracts with Blackbaud and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Blackbaud's possession and is subject to further unauthorized disclosures so long as Blackbaud fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Blackbaud's goods and services they received.

143. As a direct and proximate result of Blackbaud's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

144. Plaintiff restates and realleges all preceding allegations as if fully set forth herein.

145. Plaintiff and Class Members have an interest, both equitable and legal, in the PII conferred upon, collected by, and maintained by Blackbaud and that was stolen in the Data Breach.

146. Blackbaud benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Blackbaud understood this benefit.

147. Blackbaud also understood and appreciated that Plaintiff's and Class Members' PII was sensitive and confidential, and its value depended upon Blackbaud maintaining the privacy and confidentiality of that PII.

148. But for Blackbaud's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and trusted with Blackbaud. Indeed, if Blackbaud had informed Plaintiff and Class Members that Blackbaud's data and cyber security measures were inadequate, Blackbaud would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

149. As a result of Blackbaud's wrongful conduct, Blackbaud has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Blackbaud continues to benefit and profit from its retention and use of the PII while its value to Plaintiff and Class Members has been diminished.

150. Blackbaud's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiff's and Class Members' PII, while at the same time failing to maintain that

information secure from intrusion and theft by hackers and identity thieves.

151. Under the common law doctrine of unjust enrichment, it is inequitable for Blackbaud to be permitted to retain the benefits it received, and still receives, without justification, from Plaintiff and Class Members in an unfair and unconscionable manner. Blackbaud's retention of such benefits under the circumstances makes it inequitable, constituting unjust enrichment.

152. The benefit conferred upon, received, and enjoyed by Blackbaud was not conferred officiously or gratuitously, and it would be inequitable and unjust for Blackbaud to retain that benefit.

153. Blackbaud is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on Blackbaud as a result of its wrongful conduct, including specifically the value to Blackbaud of the PII that was stolen in the Data Breach and the profits Blackbaud is receiving from the use of that PII.

FIFTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

154. Plaintiff restates and realleges all preceding allegations as if fully set forth herein.

155. This cause of action is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

156. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Blackbaud to provide adequate security for the PII they collected from Plaintiff and Class Members.

157. Blackbaud owed a duty of care to Plaintiff and Class Members requiring them to adequately secure PII.

158. Blackbaud still possesses PII regarding Plaintiff and Class Members.

159. Since the Data Breach, Blackbaud has announced no specific changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

160. Blackbaud has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Blackbuad's insufficient data security is known to hackers, the PII in Blackbaud's possession is even more vulnerable to cyberattack.

161. Actual harm has arisen in the wake of the Data Breach regarding Blackbaud's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Blackbaud's failure to address the security failings that lead to such exposure.

162. There is no reason to believe that Blackbaud's security measures are any more adequate now than they were before the Data Breach to meet Blackbaud's contractual obligations and legal duties.

163. Plaintiff, therefore, seeks a declaration (1) that Blackbaud's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Blackbaud must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated

attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment patient data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate Plaintiff and Class Members regarding the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

SIXTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

164. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

165. At all times during Plaintiff's and Class Members' interactions with Blackbaud, Blackbaud was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Blackbaud.

166. As alleged herein and above, Blackbaud's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

167. Plaintiff and Class Members provided their respective PII to Blackbaud with the explicit and implicit understandings that Blackbaud would protect and not permit the PII to be disseminated to any unauthorized parties.

168. Plaintiff and Class Members also provided their respective PII to Blackbaud with the explicit and implicit understanding that Blackbaud would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

169. Blackbaud voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

170. Due to Blackbaud's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated

to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

171. As a direct and proximate cause of Blackbaud's actions and/or omissions, Plaintiff and Class Members have suffered damages.

172. But for Blackbaud's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Blackbaud's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

173. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Blackbaud's unauthorized disclosure of Plaintiff's and Class Members' PII. Blackbaud knew its computer systems and cyber security practices for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Blackbaud failed to observe industry standard information security practices.

174. As a direct and proximate result of Blackbaud's breaches of confidence, Plaintiff and Class Members have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

175. As a direct and proximate result of Blackbaud's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
Violation of the South Carolina Data Breach Security Act
S.C. Code Ann. §§ 39-1-90
(On Behalf of Plaintiff and the Class)

176. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

177. The South Carolina Data Breach Security Act (the "Act") requires persons conducting business in this State and owning, licensing or maintaining computerized data that includes personal identifying information to disclose breaches of the security of the system to those affected. This required disclosure "must be made in the most expedient time possible and without reasonable delay . . . ." S.C. Code Ann. § 39-1-90(A).

178. Blackbaud is a "person" as defined by the statute. S.C. Code Ann. § 39-1-90(D)(2).

179. As described more fully above, Blackbaud conducts business in this State and owns, licenses or maintains computerized data that includes personal identifying information.

180. Plaintiff's and Class Members' PII compromised in the Data Breach meets the definition of "personal identifying information" in the statute. S.C. Code Ann. § 39-1-90(D)(3).

181. The Data Breach meets the definition of "Breach of the security of the system" in the statute. S.C. Code Ann. § 39-1-90(D)(1).

182. Blackbaud violated the Act by unreasonably delaying disclosure of the Data Breach to Plaintiff and Class Members whose PII was, or was reasonably believed to have been, acquired by an unauthorized third person.

183. Blackbaud knew or should have known that it was violating South Carolina law by unreasonably delaying disclosure of the Data Breach. This renders Blackbaud's violation of the Act willful and knowing.

184. Upon information and belief, no law enforcement agency determined that notification to Plaintiff and Class Members would impede a criminal investigation.

185. As a result of Defendant's violation of the Act, Plaintiff and Class Members suffered and will continue to suffer damages and injury set forth above.

186. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, attorneys' fees, and any other relief that is just and proper.

EIGHTH CAUSE OF ACTION
Invasion of Privacy – Wrongful Publicizing of Private Affairs and Wrongful Intrusion Into Private Affairs
(On Behalf of Plaintiff and the Class)

187. Plaintiff restates and realleges all preceding allegations as if fully set forth herein.

188. Plaintiff and Class Members have a legally protected privacy interest in their protected health information which is held by Blackbaud, and they are entitled to the protection of their PII against unauthorized access.

189. Plaintiff and Class Members reasonably expected that Blackbaud would protect and secure their PII from unauthorized parties and that their PII would not be disclosed to any unauthorized parties or for any improper purpose.

190. Blackbaud unlawfully invaded the privacy rights of Plaintiff and Class Members by engaging in the conduct described above, including by failing to protect their PII, by publicizing their PII to unauthorized third parties and by unreasonably and intentionally delaying disclosure of the Data Breach.

191. This invasion of privacy resulted from Blackbaud's intentionally publicizing or causing the publication of Plaintiff's and Class Members' protected health information. This invasion of privacy also resulted from Blackbaud's intentionally intruding upon or causing the intrusion upon Plaintiff's and Class Members' PII.

192. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be from exposure, and the public has no legitimate concern in Plaintiff's and Class Members' PII.

193. Blackbaud's disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

194. Blackbaud's intentional conduct in disclosing Plaintiff's and Class Members' sensitive, personal information and delaying notification of the disclosure is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

195. The disclosure of Plaintiff's and Class Members' PII was without their consent.

196. As a result of the invasion of privacy caused by Blackbaud, Plaintiff and Class Members suffered and will continue to suffer damages and injury set forth above, including serious mental injury, shame or humiliation.

197. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of herself and all others similarly situated, prays for relief as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PII collection, storage, and protection, and to disclose with specificity to Class Members the type of PII compromised;

d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: November 19, 2020

Respectfully submitted,

By: /s/ Frank B. Ulmer

MCCULLEY MCCLUER LLC
Frank B. Ulmer
fulmer@mcculleymccluer.com
Federal ID No. 11071
Stuart H. McCluer
smccluer@mcculleymccluer.com
Federal ID No. 13213
701 E. Bay St., Ste. 411
Charleston, SC 29403
Telephone: 843-444-5404
Fax: 843-444-5408

GLANCY PRONGAY & MURRAY LLP
Brian P. Murray*
230 Park Avenue, Suite 530
New York, NY 10169
Telephone: (212) 682-5340
Facsimile: (212) 884-0988
bmurray@glancylaw.com

LAW OFFICE OF PAUL C. WHALEN, P.C.
Paul C. Whalen*
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

* *Pro Hac Vice applications to be submitted*

Attorneys for Plaintiff and the Proposed Class