UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

HELEN LOFTON, *on behalf of herself and all others similarly situated,* Plaintiff, v. BLACKBAUD, INC., Defendant.	Civil Action No.

CLASS ACTION COMPLAINT

Plaintiff, Helen Lofton, individually and on behalf of all others similarly situated, brings this action against Defendant Blackbaud, Inc. ("Blackbaud" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the May of 2020, ransomware attack and data breach ("Data Breach") of several schools, healthcare, non-profit companies, and other organizations (collectively "Clients") whose data and servers were managed, maintained, and secured by Blackbaud. The Clients' data and servers contained identifying, sensitive, and personal data from students, patients, donors, and other individual users, including Plaintiff's. As a result of the Data Breach, Plaintiff and thousands of other Class Member users suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. Additionally, Plaintiff and Class

Members' sensitive personal information—which was entrusted to Defendant, its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

2. Information compromised in the Data Breach included a copy of a subset of information retained by Blackbaud, including name(s), addresses, phone numbers, and other personal information. True and accurate copies of the notice of data breach mailed to Plaintiff ("Notice") is attached hereto, and Defendant's exemplar Notice is available on its website.[1] Contrary to the representations in the Notice regarding the type of accessed information, it is believed based on statements by Defendant's Clients directing Class Members to monitor suspicious activity of their credit and accounts, that Social Security Numbers, credit card numbers, bank account numbers, and additional personally identifiable information (collectively "Private Information") may also have been compromised. Additionally, the Notice indicates that Plaintiff's Private Health Information ("PHI"), including her medical record number, may have also been compromised.

3. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated, in order to, (1) address Defendant's inadequate safeguarding of Class Members' Private Information and PHI, which Defendant managed, maintained, and secured; (2) for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third-party; (3) for failing to identify all information that was accessed; and (4) for failing to provide Plaintiff and Class Members with any redress for the Data Breach.

4. Defendant maintained and secured the Private Information and PHI in a reckless manner, including, *inter alia*, failing to safeguard against ransomware attacks. In particular, the

[1] Blackbaud Security Incident, https://www.blackbaud.com/securityincident (last visited Sept. 16, 2020).

Private Information and PHI was maintained on, or otherwise accessible by, Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff and Class Members' Private Information and PHI was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information and PHI from those risks left that property in a dangerous condition.

5. In addition, Defendant and their employees failed to properly monitor the computer network and systems that housed the Private Information and PHI; failed to implement appropriate policies to ensure secure communications; and failed to properly train employees regarding ransomware attacks. Had Defendant properly monitored their network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Blackbaud has announced it has "already implemented changes to prevent this specific issue from happening again."[2] In other words, had these changes been in place previously, this incident would not have happened and Plaintiff and Class Members' Private Information and PHI would not have been accessed.

6. Plaintiff and Class Members' identities, Private Information, and PHI are now at risk because of Defendant's negligent conduct as the Private Information and PHI that Defendant collected and maintained was in the hands of data thieves. Defendant cannot reasonably maintain that the data thieves destroyed the subset copy simply because Defendant paid the ransom and the data thieves confirmed the copy was destroyed.

7. Armed with the Private Information and PHI accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class

[2] Blackbaud Security Incident, *supra* n.1.

members' names, taking out loans in class members' names, using Plaintiff and Class Members' names to obtain medical services, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names, but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members, at their own cost, must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Consequently, Plaintiff and Class Members will also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly-situated individuals, whose Private Information and PHI was accessed during the Data Breach.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) violation of privacy, (iii) negligence *per se*, (iv) breach of express contract, and (v) breach of implied contract, (vi) violation of state business law.

PARTIES

13. Plaintiff is a resident and citizen of Chicago, Illinois.

14. Defendant Blackbaud is a Delaware corporation with its principal place of business located on Daniel Island, Charleston County, South Carolina.

15. Defendant manages, maintains, and provides cybersecurity for the data obtained by its clients who are, *inter alia*, schools and non-profit companies, including Northwestern Medicine, which maintained Plaintiff's Private Information and PHI.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

17. This Court has personal jurisdiction over this action because Defendant has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

DEFENDANT'S BUSINESS

19. Since originally incorporating in New York in 1982,[3] Blackbaud has become "the world's leading cloud software company powering social good." This includes providing its clients with "cloud software, services, expertise, and data intelligence…" It is a publically traded company with clients that include "nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them."[4]

20. In 2019, Blackbaud reported that it had "45,000 customers located in over 100 countries," with a "total addressable market (TAM)… greater than $10 billion."[5]

21. In the ordinary course of doing business with Defendant's clients, individuals 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:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security numbers;
- Credit card account numbers;
- Bank account numbers;
- Educational history;
- Healthcare information;
- Insurance information and coverage;

[3] Blackbaud 2019 Annual Report (Feb. 20, 2020), https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417.
[4] About Blackbaud, https://www.blackbaud.com/company (last visited Sept. 18, 2020).
[5] Blackbaud 2019 Annual Report, *supra* n. 3.

- Photo identification;
- Employer information;
- Donor contribution information; and
- Other information that may be deemed necessary to provide care.

22. In its 2019 Annual Report, Blackbaud specifically addressed its known susceptibility to cyberattacks. Specifically the report states,

> ***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 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.[6]

[6] *Id*. at 19-20 (emphasis added).

23. Because of the highly sensitive and personal nature of the information Defendant maintains, manages, and secures with respect to it clients and their users, Defendant has acknowledged to their clients and users that this information will be comprehensively secured.

24. Blackbaud's Privacy Policy North America ("Privacy Policy") expressly applies 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.[7]

25. With regard to securing its constituents, supporters, patients or students of one of Defendant's customers, Defendant 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.[8]

---

[7] Blackbaud Privacy North America, https://www.blackbaud.com/company/privacy-policy/north-america (last visited August 12, 2020).
[8] *Id.*

26. Blackbaud has made additional commitments to the maintenance of student's private information. In April of 2015 with regard to its K-12 school providers, Defendant signed a pledge to respect student data privacy to safeguard student information. The Student Privacy Pledge, developed by the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA), was created to "safeguard student privacy in the collection, maintenance and use of personal information."[9]

27. In signing the Student Privacy Pledge, Blackbaud specifically represented to students and parents of its K-12 school providers that it would, *inter alia*, (1) "[m]aintain a comprehensive security program:" and (2) "[b]e transparent about collection and use of student data."[10]

28. In further support of this representation and promise to student and parent users, Travis Warrant, president of Blackbaud's K-12 Private Schools Group, stated:

> Blackbaud is committed to protecting sensitive student data and security… The Pledge will better inform our customers, service providers and the general public of our dedication to protecting student privacy." The Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.[11]

29. Despite such representations and promises, Defendant failed to adequately secure and protect numerous K-12 providers and thousands of students Private Information, by allowing the Private Information to be copied and potentially used or sold at a later date.

---

[9] Blackbaud Signs Pledge to Respect Student Data Privacy (Apr. 22, 2015), https://www.blackbaud.com/newsroom/news-archives/2015/04/22/blackbaud-signs-pledge-to-respect-student-data-privacy.

[10] *Id.*

[11] *Id.*

30. Further, due to the Health Information Portability and Accountability Act (HIPPA), Defendant had additional obligations to secure patient users' information for healthcare Clients.

31. Defendant has further failed Plaintiff and Class Members by failing to adequately secure and protect their Private Information and PHI, by allowing the Private Information and PHI to be copied and potentially used or sold at a later date.

32. Defendant further failed Plaintiff and Class Members by failing to adequately notify them of the ransomware attack or provide any remedy other than late notice.

THE CYBERATTACK AND DATA BREACH

33. Prior to the ransomware attack, clients, constituents, supporters, patients, and students provided sensitive and identifying Private Information and PHI to Blackbaud as part of, *inter alia*, seeking education from K-12 school providers and universities; seeking healthcare from healthcare providers; making donations to non-profit companies; and in other ways seeking services through Blackbaud's clients. When providing such information, these individuals had the expectation that Defendant, as the manager and securer of this Private Information and PHI, would maintain security against hackers and cyberattacks.

34. Defendant maintained Plaintiff and Class Members' Private Information and PHI on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care, schools, and other facilities over the course of recent years, Defendant did not maintain adequate security of Plaintiff and Class Members' data, to protect against hackers and cyberattacks.

35. According to its own statements, in May of 2020, Defendant discovered a ransomware attack that attempted to "disrupt business by locking companies out of their own data and servers."[12] 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 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.[13]

36. Upon information and belief, the ransomware attack began in February of 2020 and continued for approximately three months until it was stopped in May of 2020.

37. Defendant did not have a sufficient process or policies in place to prevent such cyberattack, which is evident by its own statements that it has " already implemented changes to prevent this specific issue from happening again."[14]

38. Defendant cannot reasonably rely on the word of data thieves or "certificate of destruction" issued by those same thieves, that the copied subset of any Private Information and PHI was destroyed. Further, upon information and belief, Defendant cannot be assured that Social Security numbers, Bank Account numbers, and Credit Card numbers were not also accessed and retained by the data thieves, or else it would not have advised its clients to advise

[12] Blackbaud Security Incident, *supra* n.1.
[13] *Id.*
[14] Blackbaud Security Incident, *supra* n.1.

affected individuals to monitor accounts for suspicious activity. Despite such advice, Defendant has failed to offer its clients or their users any remedy, including credit monitoring.

39. Despite having knowledge of the attack since at least May of 2020, it is believed Defendant did not notify its affected clients until July or August of 2020 of the potentially compromised data.

40. Defendant had obligations created by federal law, contracts, industry standards, common law, and privacy representations made to Plaintiff and Class Members, to keep their Private Information and PHI confidential and to protect it from unauthorized access and disclosure.

41. Plaintiff and Class Members provided their Private Information and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in its client's various industries preceding the date of the breach.

43. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. [15]

[15] Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2020), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (emphasis added).

44. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including by Defendant's own admissions in its 2019 Annual Report.

45. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Defendant's computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information and PHI;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to timely notify its Clients, Plaintiff, and Class Members of the data breach; and

e. In other such ways to be discovered.

46. As the result of Defendant's failure to take certain measures to prevent the attack until after the attack occurred, Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' Private Information and PHI.

47. Accordingly, as outlined below, Plaintiff and Class Members' daily lives were severely disrupted. Now Plaintiff and Class Members face an increased risk of fraud and identity theft.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

48. Cyberattacks and data breaches of medical facilities, schools, and non-profit entities are especially problematic because of the disruption they cause to the overall daily lives of patients, students, donors, and other individuals affected by the attack.

49. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

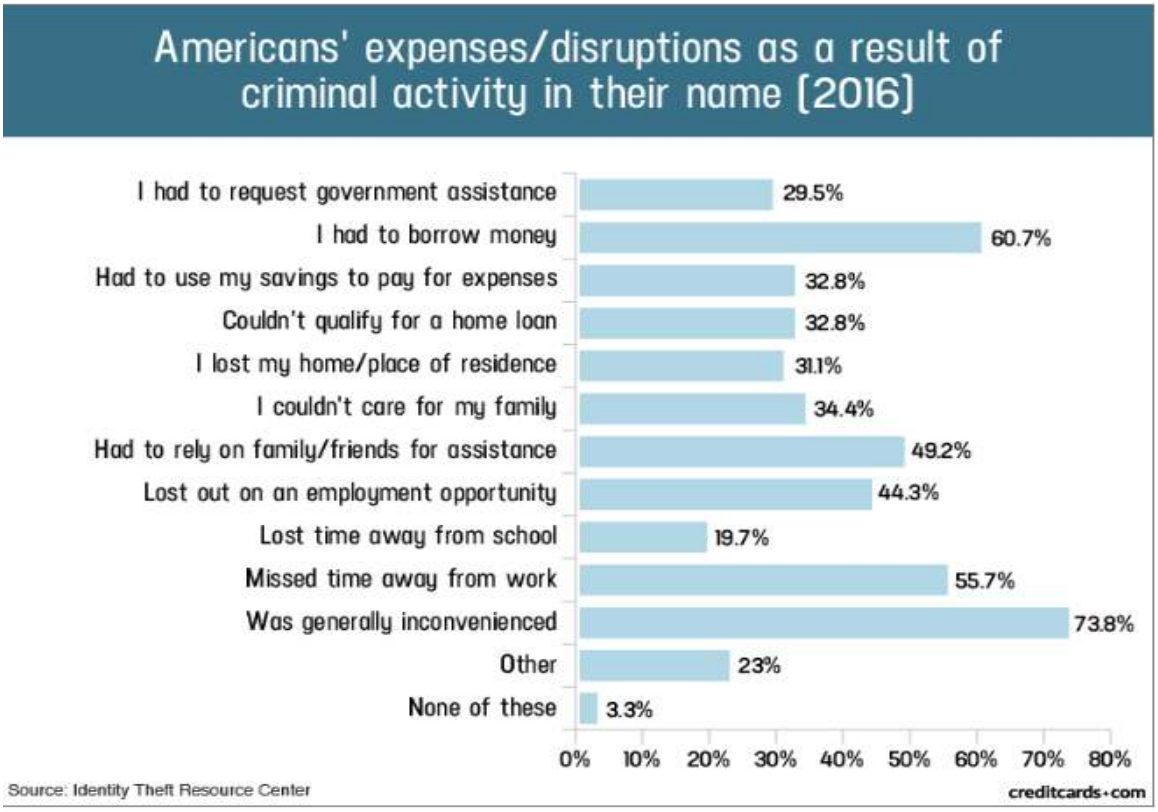
50. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

51. Identity thieves use stolen Private Information and PHI such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

52. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's

[16] *See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. Government Accountability Office Report to Congressional Requesters at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[17] *See* Federal Trade Commissions Identity Theft Steps, https://www.identitytheft.gov/Steps (last accessed Sept. 18, 2020.

Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[18]



53. Private Information and PHI is a valuable property right.[19] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information and PHI has considerable market value.

[18] Jason Steele, Credit card fraud and ID theft statistics, CreditCards.com (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[19] *See, e.g.*, John T. Soma, *et al.*, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

54. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and PHI and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report at 29.

55. Private Information, PHI, and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

56. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, as the Notices advises, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come. *See* **Exhibit A** at 6.

PLAINTIFF AND CLASS MEMBERS' DAMAGES

57. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach including, but not limited to, the costs of credit monitoring, as well as costs and loss of time they incurred because of the stolen data.

58. Plaintiff and Class Members have been damaged by the compromise of their Private Information and PHI in the Data Breach.

59. Plaintiff Helen Lofton's Private Information and PHI was compromised as a direct and proximate result of the Data Breach. While the compromise of Ms. Lofton's information was known as early as May of 2020, she did not receive a Notice until August 27, 2020. Exhibit A.

60. Like Plaintiff, other Class Members' Private Information and PHI was compromised as a direct and proximate result of the Data Breach.

61. Although the notification of the breach attempts to use language to quell Plaintiff's fears that hackers should be trusted that they destroyed the copies of Plaintiff's Private Information and PHI that was compromised, Plaintiff has no way of ever knowing if Blackbaud's payment of a ransom protected her.

62. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

63. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

64. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

65. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information and PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

66. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

67. Plaintiff and Class Members also suffered a loss of value of their Private Information and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

68. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial, student, and medical accounts and records for misuse.

69. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Like Plaintiff, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Spending additional time scrutinizing accounts for fraud and identity theft, as recommended by the breach notification;

b. Spending additional time reviewing credit reports, as recommended by the breach notification;

c. Spending additional time carefully scrutinizing electronic and other communications for types of phishing activity, which they will have to do for years to come;

d. Purchasing credit monitoring and identity theft prevention;

e. Placing "freezes" and "alerts" with credit reporting agencies, which information was provided by the breach notification;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

70. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information and PHI, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

71. Further, as a result of Defendant's conduct, Plaintiff and Class Members' Private Information and PHI—which contains the most intimate details about a person's life—is at substantial risk of disclosure, subjecting them to embarrassment and depriving them of their right to privacy.

72. As many of the purchasers of Private Information and PHI do not utilize the information for years, Plaintiff and Class Members are forced for long periods of time to endure the fear of whether their information will be used.

73. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

74. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

75. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons in the State of Illinois whose Private Information and PHI was compromised in the February through May of 2020 Data Breach described by Defendant at www.blackbaud.com/securityincident

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

76. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the class consists of approximately tens of thousands of persons whose data was compromised in Data Breach.

77. Commonality. 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 Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information and PHI;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information and PHI;

f. Whether Defendant breached their duty to Class Members to safeguard their Private Information and PHI;

g. Whether computer hackers obtained Class Members' Private Information and PHI in the Data Breach;

h. Whether Defendant knew or should have known that their data security systems and monitoring processes were deficient;

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

78. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

79. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

80. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members, as described *supra*, predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

81. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

82. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

83. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 82 above, as if fully set forth herein.

84. Defendant's Clients required Plaintiff and Class Members to submit non-public personal information in order to obtain medical, educational, and other services. Defendant had a duty to its Clients, Plaintiff, and Class Members to securely maintain the Private Information and PHI collected.

85. By accepting the duty to maintain and secure this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiff's and Class Members' Private Information and PHI held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach and/or ransomware attack.

86. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information and PHI.

87. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its Clients and Users, which is recognized by Defendants Policy Notice North America, as well as laws and regulations. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a ransomware attack and/or data breach.

88. Defendant had a specific duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

89. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information and PHI.

90. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information and PHI. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information and PHI;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information and PHI;

e. Failing to detect in a timely manner that Class Members' Private Information and PHI had been compromised; and

f. Failing to timely notify Class Members about the Ransomware Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

91. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information and PHI would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches in the Clients' various industries.

92. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information and PHI would result in one or more types of injuries to Class Members.

93. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

94. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

SECOND CLAIM FOR RELIEF
BREACH OF EXPRESS CONTRACT
(On Behalf of Plaintiff and All Class Members)

95. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 82 above, as if fully set forth herein.

96. Plaintiff and members of the Class allege that they were the direct or third-party beneficiaries of valid and enforceable express contracts, with Defendant (including, *inter alia*, Privacy Policy North America).

97. In fact, the Privacy Policy expressly extends to any "constituent, supporter, patient or student of one of [Blackbaud's] customers…"[20]

98. The valid and enforceable express contracts that Plaintiff, Class Members, and Defendant's Clients entered into with Defendant include Defendant's promise to protect Private Information and PHI given to Defendant's Clients and otherwise maintained and secured by Defendant.

[20] Blackbaud Privacy Policy *supra* n. 7.).

99. Under these express contracts, Defendant promised and were obligated to protect Plaintiff's and the Class Members' Private Information and PHI. In exchange, Defendant's Clients, Plaintiff, and members of the Class agreed to pay money for these services.

100. The protection of Plaintiff's and Class Members' Private Information and PHI were material aspects of these contracts.

101. At all relevant times, Defendant expressly represented in its Privacy Policy as follows:

> 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.[21]

102. Defendant's express representations, including, but not limited to, express representations found in its Privacy Policy, formed an express contract requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information and PHI.

103. Consumers of healthcare and education, as well as non-profit donors, value their privacy, the privacy of their dependents, and the ability to keep their Private Information and PHI associated with healthcare, education, and other institutions private. To customers such as Plaintiff and Class Members, maintenance and security of Private Information and PHI that does not adhere to industry standard data security protocols to protect Private Information and PHI is fundamentally less useful and less valuable than such services that adhere to industry-standard data security. Plaintiff and Class Members would not have given Defendant's Clients and

[21] *Id.*

Defendants their Private Information and PHI, and otherwise entered into these contracts with Defendant and/or its Clients as a direct or third-party beneficiary without an understanding that their Private Information and PHI would be safeguarded and protected.

104. A meeting of the minds occurred, as Plaintiff and members of the Class provided their Private Information and PHI to Defendant and/or its affiliated Clients, and expected protection of their Private Information and PHI.

105. Plaintiff and Class Members performed their obligations under the contract, including when they paid for services provided by Defendants' Clients or otherwise donated money.

106. Defendant materially breached its contractual obligation to protect the Private Information and PHI Defendant gathered when the information was accessed or exfiltrated by unauthorized personnel as part of the Data Breach.

107. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Policy. Defendant did not "maintain appropriate physical, electronic and procedural safeguards to protect your personal information," "protect [its] databases with various physical, technical and procedural measures and [we] restrict access to your information by unauthorized persons," or otherwise adequately train employees.

108. Defendant did not comply with industry standards, or otherwise protect Plaintiff's and the Class Members' Private Information and PHI, as set forth above.

109. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

110. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received or provided.

111. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, the Plaintiff, the Class Members, or any reasonable person would not have accepted or purchased services from Defendant and/or their Clients which required providing Private Information and PHI.

112. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information and PHI, the loss of control of their Private Information and PHI, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

113. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

THIRD CLAIM FOR RELIEF
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

114. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 82 above, as if fully set forth herein.

115. When Plaintiff and Class Members provided their Private Information and PHI to Defendant and Defendant's Clients in exchange for Defendant and Defendant's Clients' services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

116. Defendant solicited and invited Class Members to provide their Private Information and PHI as part of Defendant's regular business practices, including through its Privacy Policy. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information and PHI to Defendant.

117. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

118. Plaintiff and Class Members accepted service from, and paid money to Defendant's Clients which was conferred upon Defendant, and through which Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to maintain adequate data security. Defendant failed to do so.

119. Plaintiff and Class Members would not have entrusted their Private Information and PHI to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information and PHI to Defendant in the absence of their implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

120. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

121. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information and PHI.

122. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

123. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

124. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH CLAIM FOR RELIEF
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

125. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 82, above as if fully set forth herein.

126. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information and PHI.

127. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Private Information and PHI.

128. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable,

or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information and PHI.

129. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

130. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

131. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information and PHI.

132. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action 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 Class Members' Private Information and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for credit monitoring and identity theft protection services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: September 28, 2020

Respectfully submitted,

/s/ Amy E. Keller

Adam J. Levitt
Amy E. Keller
Brittany E. Hartwig
DiCELLO LEVITT GUTZLER LLC
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
T: 312-214-7900
Fax: 312-253-1443
Email: alevitt@dicellolevitt.com
akeller@dicellolevitt.com
bhartwig@dicellolevitt.com

Counsel for Plaintiffs and the Proposed Class Members