IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

CHRISTINA DURANKO, individually and on behalf of all others similarly situated, Plaintiff, v. BLACKBAUD, INC., Defendant.	Civil Action No. 2:20-1966 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Christina Duranko[1] ("Duranko" or "Plaintiff"), individually and on behalf of all others similarly situated, brings this class action complaint against Defendant Blackbaud, Inc. ("Blackbaud" or "Defendant") seeking monetary damages, restitution, and/or injunctive relief for herself and the Class, as defined below. Plaintiff, by and through her counsel, alleges upon personal knowledge as to herself and upon information and belief as to all other matters, based upon the investigation conducted by and through her counsel, as follows:

NATURE AND SUMMARY OF THE ACTION

1. Businesses that collect and store sensitive information about their customers, or their customers' customers, have a duty to safeguard that information and ensure it remains private. This responsibility is essential where a business keeps and stores downline consumers' Personally Identifiable Information ("PII"), such as their names, social security numbers, and dates of birth,

[1] She/Her/Hers (*see* University of Pittsburgh, Gender-Inclusivity Guidelines, available at http://www.gsws.pitt.edu/node/1432 (last visited Dec. 16, 2020)).

and Protected Health Information ("PHI"), like treatment dates, treatment locations, and other provider information.

2. Between February 7, 2020 and May 20, 2020, cyber criminals orchestrated a ransomware attack and infiltrated inadequately protected computer networks maintained by Blackbaud, a software company based in Charleston County, South Carolina, that manages, maintains, and provides cybersecurity (the "Data Breach") for several schools, healthcare, non-profit companies, and other organizations (the "Clients"). The Clients' data that was accessed contained PII and PHI (collectively, "Personal Information"), from students, patients, donors, and other individual users, including Plaintiff (the "Breach Victims"). The cyber criminals gained access to systems, which were incompetently secured by Blackbaud, and removed, among other things, Personal Information from Breach Victims.

3. Plaintiff's and all Breach Victim's sensitive Personal Information—which was entrusted to Defendant—was compromised and accessed due to the Data Breach. Information compromised and accessed in the Data Breach included a copy of a subset of information retained by Blackbaud, including full names, Social Security numbers, dates of birth, student IDs, demographic information, philanthropic giving history, usernames, passwords, bank account information, email addresses, personal and business addresses, telephone numbers, and medical information, like treatment dates, treating providers, and treatment locations. A true and accurate copy of the Data Breach notice sent to Plaintiff (the "Notice Letter") is attached hereto as **Exhibit A**, and Defendant's Data Breach notice is available on its website.[2] It is further believed, based on statements by Defendant's Clients directing Breach Victims to monitor suspicious activity of their

[2] Blackbaud, *Security Incident*, Updated Sept. 29, 2020, available at https://www.blackbaud.com/securityincident (last visited Dec. 16, 2020).

credit and accounts, that credit card numbers and additional PII was also compromised in the Data Breach.

4. In short, thanks to Defendant's gross negligence and failure to adequately protect the Breach Victims' Personal Information, cyber criminals were able to steal everything they could possibly need to commit nearly every conceivable form of identity theft and wreak havoc on the financial and personal lives of potentially hundreds of thousands of individuals.

5. Defendant caused substantial harm and injuries to Breach Victims across the United States by, *inter alia*, failing to: (1) timely implement adequate and reasonable measures to ensure Breach Victims' Personal Information was properly protected; (2) timely detect the Data Breach; (3) take adequate steps to prevent and stop the Data Breach; (4) disclose the material facts that it did not have adequate systems and security practices to safeguard Personal Information; (5) honor its repeated promises and representations to protect the Breach Victims' Personal Information; (6) identify all information that was accessed; (7) maintain its computer network in a condition to protect against ransomware attacks or other cyberattacks; (8) provide timely and adequate notice of the Data Breach; (9) properly monitor the computer network and systems that housed Breach Victims' Personal Information; (10) implement appropriate policies to ensure secure communications; (11) properly train employees regarding ransomware attacks; and (12) provide Plaintiff and the Breach Victims with any redress for the Data Breach.

6. Had Defendant properly monitored its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Blackbaud announced it has "already implemented changes to prevent this specific issue from happening

again."[3] In other words, had these changes been in place earlier, this incident would not have happened and Plaintiff and Class members' Personal Information would not have been compromised.

7. As a result of Defendant's conduct, Breach Victims suffered damages. For example, when Plaintiff discovered her Personal Information was compromised, she became anxious and stressed. The Data Breach was particularly concerning to Plaintiff because Defendant has compromised her medical history and patient files. To this end, Plaintiff worries not only about her medical history being stolen, but also manipulated. The consequences would be devastating because Plaintiff's future medical treatment would rely on inaccurate medical and treatment histories. Plaintiff undergoes treatment for many issues from many providers. Now, as a result of the Data Breach, Plaintiff must vigorously confirm each provider's treatment recommendations rely on her correct medical history, thereby making every appointment even more stressful than they were before the Data Breach. Plaintiff has also been spending time continuously monitoring her financial accounts for suspicious activity to ensure that her very high credit rating—which Plaintiff has worked very hard to achieve—will not take a massive hit due to cyber thieves improperly using her Personal Information as a result of the latest Data Breach of which she's been a victim. She has also spent time contacting Allegheny Health Network's Chief Privacy Officer concerning the disclosure and distribution of her Personal Information and to request an accounting of the information stolen. Although Defendant has not yet indicated that Plaintiff's driver's license number was compromised in the Data Breach, Plaintiff is considering changing it anyway now that her PHI has been compromised and will likely be added to whatever other information hackers

[3] *Id.*

have aggregated as to Plaintiff from other data breaches. Finally, since the Data Breach, Plaintiff has also experienced spam emails, text messages, and phone calls.

8. Now that their Personal Information has been released into the criminal cyber domains, Plaintiff and all Breach Victims are at imminent risk of identity theft. This risk—caused by Defendant's failures—will continue to exist for years to come, and Breach Victims must spend their time being extra vigilant to avoid being victimized for the rest of their lives.

9. Plaintiff brings this lawsuit as a class action on behalf of a proposed Class to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or reasonable cybersecurity measures to protect Class members' Personal Information.[4]

10. Because Defendant presented such a soft target to cyber criminals, Plaintiff and Class members have already been subjected to violations of their privacy, fraud, and identity theft, or have been exposed to a heightened and imminent risk of certainly impending fraud and identity theft. Plaintiff and Class members must now, and in the future, spend time to closely monitor their financial and medical accounts to guard against identity theft.

11. As a result of the Data Breach, Plaintiff and other Class members suffered ascertainable losses and may also be required to incur out-of-pocket costs for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to remedy or mitigate the effects of the attack.

12. On behalf of herself and all Breach Victims, Plaintiff seeks actual damages, statutory damages, and punitive damages, with attorneys' fees, costs, and expenses, and asserts claims for: (i) negligence; (ii) intrusion upon seclusion; (iii) negligence *per se*; (iv) breach of

[4] References to "members of the Class," "Class members," and "Breach Victims" are used interchangeably herein.

express contract; (v) breach of implied contract; and (vi) violations of state data breach statutes. Plaintiff also seeks injunctive relief, including significant improvements to Defendant's data security systems, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

PARTIES

13. Plaintiff is a citizen and resident of Whitaker, Pennsylvania, in Allegheny County.

14. Defendant is a Delaware corporation with its principal place of business located on Daniel Island, Charleston County, South Carolina. Defendant manages, maintains, and provides cybersecurity for the data obtained by its Clients who are, *inter alia*, schools and non-profit companies, including Allegheny Health Network, which maintained Plaintiff's Personal Information.

JURISDICTION AND VENUE

15. 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

16. 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.

17. The claims alleged arise under Title III such that this Court's jurisdiction is invoked pursuant to 28 U.S.C. § 1331 and 42 U.S.C. § 12188.

18. Venue in this District is proper under 28 U.S.C. § 1391(b)(2) because this is the judicial district in which a substantial part of Plaintiff's injuries occurred.

FACTUAL ALLEGATIONS

A. Defendant Blackbaud, Inc.

19. Since originally incorporating in 1982,[5] 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 publicly traded company with Clients that include "nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them."[6]

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."[7]

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 private information includes or may include the following personal data without limitation: name, address, phone number and email address; date and place of birth; demographic information; Social Security numbers; credit card account numbers; bank account numbers; educational history; healthcare records or information; insurance information and coverage; photo identification; employer information; donor contribution information; and usernames and passwords.

---

[5] Blackbaud, Inc., Annual Report (Form 10-K) (Feb. 20, 2020), available at https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417 (last visited Dec. 16, 2020).

[6] Blackbaud, https://www.blackbaud.com/company (last visited Dec. 16, 2020).

[7] *See supra* note 5.

22. Prior to the ransomware attack, Clients provided sensitive and identifying private information 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, would maintain reasonable security to thwart hackers and cyberattacks.

B. The Data Breach

23. Defendant inadequately maintained Plaintiff and Class members' Personal Information on a shared network, server, and/or software. As explained below, Defendant did not have sufficient processes or policies in place to prevent a cyberattack, which allowed cyber criminals to access and remove Plaintiff and Class members' highly sensitive data.

24. In July of 2020, Blackbaud posted a "security incident" notification on its website, disclosing, for the first time, that in May of 2020 cybercriminals had accessed and "removed a copy of a subset of data from [Blackbaud's] self-hosted environment." Blackbaud claimed the "cybercriminal did not access credit card information, bank account information, or social security numbers," and, "[b]ecause protecting our customers' data is our top priority," Blackbaud "paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed."

25. Subsequently, Blackbaud changed its "security incident" notification and noted that "[f]or those customers where Blackbaud directly communicated involvement in the security incident," "the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords."[8]

[8] *See supra* note 2.

26. Allegheny Health Network, one of Blackbaud's Clients, also sent Plaintiff a Notice Letter, dated December 4, 2020, stating, in part:

> …Prior to blocking the attack, however, the attacker was able to obtain a copy of some customer data belonging to several of Blackbaud's clients, including the AHN Office of Development.
>
> …
>
> Data accessed by the attacker may have contained your name, date of birth, address, busines address, phone numbers, e-mail addresses, and limited medical information, such as dates you may have had services provided at AHN, your treating provider's name, and the AHN location.
>
> …
>
> AHN will continue to monitor the situation closely with Blackbaud. We have determined that notice to you is appropriate as there was an inappropriate acquisition of your personal information during a ransomware attack on Blackbaud's system.[9]

27. Upon information and belief, Blackbaud also sent notices to other Clients directing them to notify other Breach Victims to monitor suspicious activity of their credit and accounts.

28. This means that the cyber criminals had unrestricted access to ***unencrypted*** Personal Information of Plaintiff and all Breach Victims for at least three months, and that Blackbaud did not notify its Clients about the Data Breach until months after it purportedly learned of the Data Breach—unreasonable delays under any objective measure.

29. Blackbaud apparently chose to complete its internal investigation and develop its excuses and speaking points before giving Class members the information it needed to protect themselves against fraud and identity theft.

30. This was a staggering coup for the cyber criminals and a stunningly bad showing

[9] *See* Exhibit A.

for Defendant.

31. In spite of the severity of the Data Breach, Defendant has done nothing to protect the Breach Victims.

32. Blackbaud failed to adequately safeguard Plaintiff and Class members' Personal Information, allowing cyber criminals to access this wealth of priceless information for over three months, and then use it for another two months before Blackbaud warned the criminals' victims—the Breach Victims—to be on the lookout. Indeed, Blackbaud evidently failed to spend sufficient resources on monitoring its systems and training its employees to identify threats and defend against them.

33. Plaintiff and Class members provided their Personal Information 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.

34. Defendant had obligations and duties created by state and federal law, contracts, industry standards, common law, and privacy representations made to Plaintiff and Class members, to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

35. As discussed below, Defendant was well aware of its obligation to keep Personal Information confidential and to protect the information from unauthorized access.

C. Defendant Expressly Understood That It Was Obligated To Safeguard Personal Information

36. Because of the highly sensitive and personal nature of the information Defendant maintains, manages, and secures with respect to its Clients, Defendant has acknowledged to its Clients that this information will be comprehensively secured.

37. 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.[10]

38. 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.[11]

39. Notwithstanding the foregoing understanding, Blackbaud failed to protect the Personal Information of Plaintiff and other Class members from cyber criminals who were able to use a ransomware attack to extract valuable information from Blackbaud's self-hosted systems.

---

[10] Blackbaud, *Privacy Policy North America*, available at https://www.blackbaud.com/company/privacy-policy/north-america (last visited Dec. 16, 2020).

[11] *Id.*

40. Defendant's data security obligations were particularly important given the well-known substantial increase in data breaches in the healthcare industry, including the recent massive data breach involving LabCorp, Quest Diagnostics, and American Medical Collections Agency. When considering the wide publicity as to these data breaches, there is no excuse for Blackbaud's failure to adequately protect Plaintiff's and Class members' Personal Information.

41. That sensitive information is now in the hands of cyber criminals who will use it if given the chance. Much of this information is immutable and loss of control over this information is remarkably dangerous to consumers.

42. Further, Blackbaud is an entity covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (45 C.F.R. §160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

43. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

44. HIPAA's Security Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is created, received, used, or maintained in electronic form.

45. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information. " 45 C.F.R. §164.302.

46. "Electronic protected health information" is "individually identifiable health

information . . . that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media…" 45 C.F.R. §160.103.

47. HIPAA's Security Rule requires Defendant to do the following:

(a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

(b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(c) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

(d) Ensure compliance by its workforce.

48. HIPAA also requires Defendant to "review and modify the security measures implemented…as needed to continue provision of reasonable and appropriate protection of electronic protected health information " 45 C.F.R. §164.306(e).

49. HIPAA also requires Defendant to "[i]mplement 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 " 45 C.F.R. §164.312(a)(1).

50. The HIPAA Breach Notification Rule, 45 C.F.R. §§164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[12]

51. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act")

[12] Breach Notification Rule, U.S. DEP'T OF HEALTH & HUMAN SERVS., available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Dec. 16, 2020).

(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).

52. Moreover, Defendant had obligations and duties created by state and federal law, contracts, industry standards, common law, and privacy representations made to Plaintiff and Class members, to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

53. In addition to its obligations under federal and state laws, Defendant owed a duty to Breach Victims whose Personal Information it managed, monitored, and secured to:

(a) exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons;

(b) to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of the Breach Victims;

(c) to design, maintain, and test its systems to ensure that the Personal Information in Defendant's possession was adequately secured and protected;

(d) to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees and others who accessed the information within its systems on how to adequately protect Personal Information;

(e) to implement processes that would detect a breach of its data security systems in a timely manner;

(f) to act upon data security warnings and alerts in a timely fashion;

(g) to disclose the fact that its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant; and

(h) to disclose in a timely and accurate manner when data breaches occurred

54. Defendant owed a duty of care to Breach Victims because they were foreseeable and probable victims of any inadequate data security practices.

D. Defendant Was On Notice Of Cyberattack Threats And The Inadequacy Of Its Data Security.

55. In its 2019 Annual Report, Blackbaud specifically addressed its known susceptibility to cyberattacks:

> 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**.
>
> 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[.]**
>
> 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.[13]

56. Defendant was also on notice that the Federal Bureau of Investigation ("FBI") has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack

[13] *See supra* note 5 (emphasis added).

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)."[14]

57. Indeed, cyberattacks have become so notorious that as recently as November 2019, the FBI and U.S. Secret Service issued warnings to potential targets so they are aware of, and prepared for, a potential attack.[15]

58. 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.[16]

59. Despite knowing that cyberattacks were prevalent, and admitting its security system was vulnerable to such attacks, Defendant failed to implement sufficient safeguards to secure and protect Plaintiff's and Class members' Personal Information. Instead, it allowed the Personal Information to be accessed by cybercriminals, copied, removed, and potentially used or sold at a later date.

E. A Data Breach Like Blackbaud's Results In Debilitating Injury To Consumers

60. Each year, identity theft causes tens of billions of dollars of losses to victims in the

---

[14] 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 visited Dec. 16, 2020).

[15] Ben Kochman, *FBI, Secret Service Warn Of Targeted Ransomware*, LAW 360 (Nov. 18, 2019), available at https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Dec. 16, 2020).

[16] *See supra* note 5.

United States.[17] Cyber criminals can leverage Plaintiff's and Class members' Personal Information that was stolen in the Data Breach to commit thousands or millions of additional crimes, including opening new financial accounts in Breach Victims' names, taking out loans in Breach Victims' names, using Breach Victims' names to obtain medical services and government benefits, using Breach Victims' Personal Information to file fraudulent tax returns, using Breach Victims' health insurance information to rack up massive medical debts in their names, using Breach Victims' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Breach Victims' information to obtain government benefits, filing fraudulent tax returns using Breach Victims' information, obtaining driver's licenses in Breach Victims' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Breach Victims could be arrested for crimes identity thieves have committed.

61. This was a financially motivated Data Breach, as the only reason the cyber criminals stole Plaintiff's and the Class members' Personal Information from Blackbaud was to engage in the kinds of criminal activity described above, which will result, and has already begun to, in devastating financial and personal losses to Breach Victims.

62. This is not just speculative. As the FTC has reported, if hackers get access to Personal Information, they ***will*** use it.[18]

63. Hackers may not use the information right away. According to the U.S.

---

[17] *Facts + Statistics: Identity theft and cybercrime*, INS. INFO. INST. (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity"), available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Dec. 16, 2020).

[18] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), available at https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited Dec. 16, 2020).

Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[19]

64. For instance, with a stolen social security number, which is part of the Personal Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[19] Identity thieves can also use the information stolen from Breach Victims to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

65. "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."[20]

66. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI can go from $20 say up to—we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[21] A complete identity theft kit that includes

---

19 *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFFICE (July 5, 2007) (emphasis added), available at https://www.gao.gov/products/GAO-07-737 (last visited Dec. 16, 2020).

20 *Id.*

21 IDX, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows* (May 14, 2015), previously available at https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-data.

health insurance credentials may be worth up to $1,000 on the black market.[22]

67. If, moreover, the cyber criminals also manage to steal financial information, such as credit and debit cards—as they did here—there is no limit to the amount of fraud that the Breach Victims have exposed to resulting from Blackbaud's ineptitude.

68. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[23]

69. 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.[24]

70. Private information is a valuable property right.[25] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts, including heavy prison sentences. This obvious risk to reward analysis illustrates that Personal Information has

---

[22] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015 (Sept. 30, 2014), available at https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Dec. 16, 2020).

[23] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), available at https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Dec. 15, 2020).

[24] *Steps*, FED. TRADE COMM'N, available at https://www.identitytheft.gov/Steps (last visited Dec. 16, 2020).

[25] *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).

considerable market value.

71. Personal 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.

72. 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, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

F. Plaintiff's And Class Member's Damages

73. Plaintiff and other Breach Victims have already experienced the risks and harms discussed above.

74. Plaintiff's experience is not unique to those of other Breach Victims, as Plaintiff's Personal Information was exposed in the same Data Breach to the same malicious actors.

75. 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 data breach.

76. The Personal Information of Plaintiff was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May 2020, Plaintiff did not receive Notice until December 4, 2020. *See* Exhibit A.

77. When Plaintiff discovered her Personal Information was compromised, she became anxious and stressed. The Data Breach was particularly concerning to Plaintiff because

Defendant has compromised her medical history and patient files. To this end, Plaintiff worries not only about her medical history being stolen, but also manipulated. The consequences would be devastating because Plaintiff's future medical treatment would rely on inaccurate medical and treatment histories. Plaintiff undergoes treatment for many issues from many providers. Now, as a result of the Data Breach, Plaintiff must vigorously confirm each provider's treatment recommendations rely on her correct medical history, thereby making every appointment even more stressful than they were before the Data Breach. Plaintiff has also been spending time continuously monitoring her financial accounts for suspicious activity to ensure that her very high credit rating—which Plaintiff has worked very hard to achieve—will not take a massive hit due to cyber thieves improperly using her Personal Information as a result of the latest Data Breach of which she's been a victim. She has also contacted Allegheny Health Network's Chief Privacy Officer concerning the disclosure and distribution of her Personal Information and to request an accounting of the information stolen. Although Defendant has not yet indicated that Plaintiff's driver's license number was compromised in the Data Breach, Plaintiff is considering changing it anyway now that her PHI has been compromised and will likely be added to whatever other information hackers have aggregated as to Plaintiff from other data breaches. Finally, since the Data Breach, Plaintiff has also experienced spam emails, text messages, and phone calls.

78. Like Plaintiff, other Class members' Personal Information was compromised and accessed as a direct and proximate result of the Data Breach.

79. 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 for fraud and identity theft.

80. 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.

81. 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.

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

83. 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.

84. Plaintiff and Class members also suffered a loss of value of their Personal Information 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.

85. 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.

86. 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) Finding fraudulent charges;

(b) Canceling and reissuing credit and debit cards;

(c) Purchasing credit monitoring and identity theft prevention;

(d) Addressing their inability to withdraw funds linked to compromised accounts;

(e) Taking trips to banks and waiting in line to obtain funds held in limited accounts;

(f) Placing "freezes" and "alerts" with credit reporting agencies;

(g) Spending time on the phone with or at a financial institution to dispute fraudulent charges;

(h) Contacting financial institutions and closing or modifying financial accounts;

(i) Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

(j) 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

(k) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

87. Moreover, Plaintiff and Class members have an interest in ensuring that their Personal Information, 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.

88. Further, as a result of Defendant's conduct, Plaintiff and Class members are forced to live with the knowledge that their Personal Information—which contains the most intimate details about their lives—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of their fundamental right to privacy.

89. As many of the purchasers of Personal Information 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.

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

CLASS ACTION ALLEGATIONS

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

92. Plaintiff proposes the following Class definition, subject to amendment and subclasses as appropriate

> All individuals residing in the Commonwealth of Pennsylvania whose Personally Identifiable Information or Private Health Information was compromised as a result of the Blackbaud Data Breach.

93. 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.

94. **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, or possibly hundreds of thousands, of persons and entities whose data was compromised in the Data Breach.

95. **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' Personal Information;

(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 Personal Information;

(f) Whether Defendant breached its duty to Class members to safeguard their Personal Information;

(g) Whether computer hackers obtained, sold, copied, stored, or released Class members' Personal Information;

(h) Whether Defendant knew or should have known that its 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 actions, 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.

96. **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.

97. **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.

98. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that Plaintiff's and Class members' Personal Information was stored on the same computer systems and were unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class members, as described above, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

99. **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.

100. 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.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

101. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint to the extent they are not inconsistent with the allegations of this Count I.

102. In *Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018), the Pennsylvania Supreme Court held that "an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system." *Id* at 1038. In reaching this decision, the Court explained:

> Again, Employees allege that UPMC, their employer, undertook the collection and storage of their requested sensitive personal data without implementing adequate security measures to protect against data breaches, including encrypting data properly, establishing adequate firewalls, and implementing adequate authentication protocol. The alleged conditions surrounding UPMC's data collection and storage are such that a cyber-criminal might take advantage of the vulnerabilities in UPMC's computer system and steal Employees' information; thus, the data breach was "within the scope of the risk created by" UPMC. *See Ford*, 379 A.2d at 115 (explaining that the dilapidated condition of the appellee's property, which had caught fire and damaged the appellant's neighboring property, "was such that third persons might avail themselves of the opportunity to commit a tort or crime" and that "such acts were within the scope of the risk created by the appellee"). Therefore, the criminal acts of third parties in executing the data breach do not alleviate UPMC of its duty to protect Employees' personal and financial information from that breach.

Id. at 1048.

103. Like the employees of UPMC, 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 Personal Information collected as promised and warranted.

104. By accepting the duty to maintain and secure this data in its computer systems, 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 systems—and Plaintiff's and Class members' Personal Information held within it—to prevent disclosure of the information, and to protect the information from cyber theft. Defendant's duty included a responsibility to implement processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a data breach and/or ransomware attack.

105. 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 and safeguarded the Personal Information of the Class.

106. 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 Defendant's Privacy Policy, 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.

107. Defendant had a specific duty to employ reasonable security measures under Section 5 of the FTC 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.

108. 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 Personal Information.

109. Defendant breached its duties, and thus was negligent, by failing to use reasonable

measures to protect Class members' Personal Information. 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' Personal Information;

(b) Failing to adequately monitor the security of its networks and systems;

(c) Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

(d) Allowing unauthorized access to Class members' Personal Information;

(e) Failing to detect in a timely manner that Class members' Personal Information had been compromised; and

(f) Failing to timely notify Class members about the Data Breach and ransomware attack so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages

110. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Personal Information 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.

111. It was therefore foreseeable that the failure to adequately safeguard Class members' Personal Information would result in one or more types of injuries to Class members.

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

113. 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, and any other relief this Court deems just and proper.

COUNT II
INVASION OF PRIVACY

114. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint to the extent they are not inconsistent with the allegations of this Count II.

115. The Commonwealth of Pennsylvania recognizes the tort of invasion of privacy and the Supreme Court of Pennsylvania has indicated that it consists of "an intentional intrusion on the seclusion of their private concerns which was substantially and highly offensive to a reasonable person, and aver sufficient facts to establish that the information disclosed would have caused mental suffering, shame or humiliation to a person of normal sensibilities." *ProGolf Mfg., Inc. v. Tribune Rev. Newspaper Co.*, 570 Pa. 242, 247 (2002).

116. Plaintiff and Class members had a reasonable expectation of privacy, and freedom from exposure, in the Personal Information that Defendant mishandled.

117. Defendant's conduct as alleged above intruded upon Plaintiff's and Class members' private aspects under common law.

118. Defendant's intrusion was substantial and unreasonable enough to be legally cognizable, in that the reasonable expectation of persons of normal and ordinary sensibilities, including Plaintiff, is that the Personal Information entrusted to Defendant's Clients would be properly maintained and secured.

119. By failing to keep Plaintiff's and Class members' Personal Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiff's and Class members' privacy by:

(a) Substantially intruding into Plaintiff's and Class members' private affairs in a manner that identifies Plaintiff and Class members and that would be highly offensive and objectionable to an ordinary person;

(b) Negligently publicizing private facts about Plaintiff and Class members, which is highly offensive and objectionable to an ordinary person; and

(c) Negligently causing anguish or suffering to Plaintiff and Class members.

120. Defendant knew that an ordinary person in Plaintiff's or a Class member's position would consider Defendant's intentional actions highly offensive and objectionable.

121. Defendant invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their Personal Information without their informed, voluntary, affirmative, and clear consent.

122. Defendant concealed from Plaintiff and Class members an incident that misused and/or disclosed their Personal Information without their informed, voluntary, affirmative, and clear consent.

123. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's actions or inaction highly offensive and objectionable.

124. In failing to protect Plaintiff's and Class members' Personal Information, and in misusing and/or disclosing their Personal Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of Plaintiff and the Class.

COUNT III
BREACH OF PHYSICIAN-PATIENT CONFIDENTIALITY

125. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint

to the extent they are not inconsistent with the allegations of this Count III.

126. In addition to the tort of invasion of privacy, the Commonwealth of Pennsylvania recognizes the tort of breach of physician-patient confidentiality and the Superior Court of Pennsylvania has indicated that it occurs where "confidential disclosures [of patient information] occurred that were unrelated to any judicial proceedings." *Burger v. Blair Med. Assocs.*, 2007 PA Super. 164, ¶ 12, 928 A.2d 246, 249 (Pa. Super. 2007).

127. Plaintiff and Class members had a reasonable expectation of privacy, and freedom from exposure, in the PHI that Defendant mishandled.

128. Defendant's conduct as alleged above intruded upon Plaintiff's and Class members' private aspects under common law.

129. Defendant's intrusion was substantial and unreasonable enough to be legally cognizable, in that the reasonable expectation of persons of normal and ordinary sensibilities, including Plaintiff, is that the PHI entrusted to Defendant's Clients would be properly maintained and secured.

130. By failing to keep Plaintiff's and Class members' PHI safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant breached the physician-patient confidentiality obligations it owed Plaintiff and Class members by causing their PHI to be disclosed unrelated to judicial proceedings.

131. Defendant knew that an ordinary person in Plaintiff's or a Class member's position would consider Defendant's intentional actions highly offensive and objectionable.

132. Defendant concealed from Plaintiff and Class members an incident that misused and/or disclosed their PHI without their informed, voluntary, affirmative, and clear consent.

133. As a proximate result of such misuse and disclosures, Plaintiff's and Class

members' reasonable expectations of privacy in their PHI was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's actions or inaction highly offensive and objectionable.

134. In failing to protect Plaintiff's and Class members' PHI, and in misusing and/or disclosing their PHI, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of Plaintiff and the Class.

COUNT IV
BREACH OF EXPRESS CONTRACT

135. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint to the extent they are not inconsistent with the allegations of this Count IV.

136. 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*, the Privacy Policy).

137. In fact, Plaintiff's Privacy Policy expressly extends to any "constituent, supporter, patient or student of one of [Blackbaud's] customers[.]"[26]

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

139. Under these express contracts, Defendant promised and were obligated to protect Plaintiff's and the Class members' Personal Information. In exchange, Defendant's Clients,

[26] *See supra* note 10.

Plaintiff, and members of the Class agreed to pay money for these services.

140. The protection of Plaintiff's and Class members' Personal Information were material aspects of these contracts.

141. At all relevant times, Defendant expressly represented in its Privacy 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.

142. 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' Personal Information.

143. 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 Personal Information associated with healthcare, education, and other institutions private. To customers such as Plaintiff and Class members, maintenance and security of Personal Information that does not adhere to industry standard data security protocols to protect Personal Information 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 Defendant their Personal Information, and otherwise entered into these contracts with Defendant and/or its Clients as a direct or third-party beneficiary without an understanding that their Personal Information would be safeguarded and protected.

144. A meeting of the minds occurred, as Plaintiff and members of the Class provided

their Personal Information to Defendant and/or its affiliated Clients, and expected protection of such information.

145. Plaintiff and Class members performed their obligations under the contract, including when they paid for services provided by Defendant's Clients or otherwise donated money.

146. Defendant materially breached its contractual obligation to protect the Personal Information Defendant gathered when the information was accessed or removed by unauthorized personnel as part of the Data Breach.

147. 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 [the] personal information," "protect [its] databases with various physical, technical and procedural measures and…restrict access to [the] information by unauthorized persons," or otherwise adequately train employees.

148. Defendant did not comply with industry standards, or otherwise protect Plaintiff's and the Class members' Personal Information, as set forth above.

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

150. 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.

151. 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 its Clients which required providing Personal Information.

152. 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 Personal Information, the loss of control of their Personal Information, 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.

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

COUNT V
BREACH OF IMPLIED CONTRACT

154. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint to the extent they are not inconsistent with the allegations of this Count V.

155. When Plaintiff and Class members provided their Personal Information 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.

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

Defendant.

157. 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.

158. 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.

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

160. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendant

161. Defendant breached its implied contracts with Class members by failing to safeguard and protect their Personal Information.

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

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

164. 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.

COUNT VI
NEGLIGENCE *PER SE*

165. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint to the extent they are not inconsistent with the allegations of this Count VI.

166. Pursuant to the FTC 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' Personal Information.

167. 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' Personal Information.

168. Defendant breached its duties to Plaintiff and Class members under the FTC 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' Personal Information.

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

170. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff's and Class members' Personal Information would not have been stolen and they would not have been harmed.

171. 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 Personal Information, including increased risk of identity theft.

172. 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.

COUNT VII
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Const. Stat. §§ 201-2 & 201-3, *et seq.*

173. Plaintiff re-alleges and incorporates by reference all Paragraphs of this Complaint to the extent they are not inconsistent with the allegations of this Count VII.

174. Plaintiff and Defendant are each a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

175. Plaintiff and Class Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

176. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of their trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including, but not limited to, the following:

(a) Representing that their goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

(b) Representing that their goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

(c) Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

177. Defendant's unfair or deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Personal Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Personal Information; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

178. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

179. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

180. Had Defendant disclosed to Plaintiff and Class Members that its data systems were

not secure and thus vulnerable to attack, Defendant would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure and was trusted with sensitive and valuable Personal Information regarding thousands of consumers, including Plaintiff and the Class members.

181. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of their security controls secret from the public.

182. Plaintiff and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

183. Defendant acted intentionally, knowingly, and maliciously to violate the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff's and Class Members' rights. Past data breaches and ransomware attacks in the healthcare industry put Defendant on notice that its security and privacy protections were inadequate.

184. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Class members' reliance on them, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from disruption of medical care and treatment; fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

185. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests 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' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members or to mitigate further harm;

(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 Personal Information 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 not less than seven years of credit monitoring 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 reasonable 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: December 18, 2020

/s/ Kevin Tucker

Kevin W. Tucker (He/Him/His)
Pa. No. 312144
Kevin J. Abramowicz
Pa. No. 320659
EAST END TRIAL GROUP LLC
6901 Lynn Way, Suite 215
Pittsburgh, PA 15208
Tel. (412) 877-5220
Fax. (412) 626-7101
ktucker@eastendtrialgroup.com
kabramowicz@eastendtrialgroup.com

Stuart A. Davidson (*pro hac vice* forthcoming)
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Tel. (561) 877-5220
Fax. (561) 626-7101
sdavidson@rgrdlaw.com

Desiree Cummings (*pro hac vice* forthcoming)
ROBBINS GELLER RUDMAN & DOWD LLP
420 Lexington Avenue, Suite 1832
New York, NY 10170
Tel. (212) 693-1058
dcummings@rgrdlaw.com

Counsel for Plaintiff