MARC M. SELTZER (54534)
mseltzer@susmangodfrey.com
KRYSTA KAUBLE PACHMAN (280951)
kpachman@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067-6029
Phone: (310) 789-3100
Fax: (310) 789-3150

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

PHILIP EISEN, on behalf of himself and all others similarly situated, Plaintiff, vs. BLACKBAUD, INC., Defendant.	Case No: **CLASS ACTION** **COMPLAINT FOR DAMAGES AND DECLARATORY RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiff, by and through his attorneys, complains and alleges as follows:

INTRODUCTION

1. Defendant Blackbaud, Inc. ("Blackbaud") provides internet cloud software, services expertise and data intelligence to thousands of nonprofits, foundations, corporations, educational institutions, healthcare institutions and individual change agents.

2. Blackbaud was the subject of a massive data breach that began on or about February 7, 2020. Blackbaud did not detect the breach for three months, when Blackbaud personnel noticed a suspicious log-in on an internal server on May 14, 2020. The hacker was able to remove a copy of a "subset of data" from Blackbaud's self-hosted environment. According to Blackbaud, the hacker's activity and attempts to regain access continued until June 3, 2020. The Blackbaud hacker contacted Blackbaud with a Bitcoin ransom demand and provided a statement of involved files on June 18, 2020. Blackbaud ultimately paid the hacker a ransom in an undisclosed amount of Bitcoin and told its customers that the hacker represented that the stolen data was destroyed based on payment of the ransom.

3. Rather than provide its customers with information about the breach as soon as it claims it learned about it so that they could notify consumers whose personal information had been provided to it, Blackbaud did not begin telling its customers of the data breach until July 16, 2020. Those customers, which include prominent organizations like Harvard University, Planned Parenthood, and National Public Radio, have been sending out individual notices advising consumers that their personal information may have been compromised, including, *inter alia*, their name, title, date of birth, gender, student ID number, phone number, email address, LinkedIn profile URL, course and educational details, records of fundraising activities and donations, professional details, spouse's identity, estimated net worth and identified assets, giving history to other charities and other nonprofit organizations, likelihood to make a bequest upon their death, events attended, and

friend connections. Although Blackbaud initially represented to its customers that "the cybercriminal did not access credit card information, bank account information, or social security numbers," Blackbaud customers have subsequently learned that the hacker accessed sensitive personal information, including social security numbers, driver's license numbers, medical information, and passport numbers, that was not encrypted.

4. Blackbaud has acknowledged that there was an undetected vulnerability that led to the breach. Blackbaud has refused to provide any further information regarding the undetected vulnerability. Upon information and belief, the undetected vulnerability and subsequent breach were the result of substandard data security practices.

5. Upon information and belief, the hacker did not, as promised, destroy the personal information obtained in the data breach, and plaintiff and the Class are at risk that identity thieves will commit a variety of crimes, such as taking out loans, mortgaging property, opening financial accounts in a victim's name, opening credit card accounts in a victim's name, using a victim's information to obtain government benefits, filing fraudulent tax returns to obtain a tax refund, obtaining a driver's license or identification card in a victim's name, gaining employment in a victim's name, obtaining medical services in a victim's name, or giving false information to police. Hackers also commonly sell personal information to other criminals who, in turn, misuse the information for fraudulent purposes.

6. As a result of Blackbaud's negligent failure to prevent the data breach, plaintiff and the Class face a heightened, imminent risk of such harm in the future. Plaintiff and the Class must now incur the expense and inconvenience of monitoring their financial accounts and credit histories to guard against the increased risk of identity theft, and will incur out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the data breach's impact on their lives.

7. Blackbaud has failed to offer credit monitoring or any other services to consumers adversely affected by the data breach.

8. This is a class action brought on behalf of a nationwide Class of persons whose information was accessed as a result of Blackbaud's negligent failure to adequately protect individuals' personal information, failure to warn its clients and the persons whose personal information was entrusted to Blackbaud of its inadequate information security practices, and failure to effectively monitor its platform for security vulnerabilities. Plaintiff brings causes of action for negligence, violation of South Carolina's Data Breach Security Act, S.C. Code Ann. §§ 39-1-90, *et seq*., violation of South Carolina's Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10, *et seq*., and breach of contract. Plaintiff also brings this action on behalf of a subclass of consumers residing in California for violation of California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, violation of California's Customer Records Act, Cal. Civil Code §§ 1798.80, *et seq*., and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200.

9. Plaintiff seeks damages stemming from at least the following:

a. Loss of value of personal information;

b. Out-of-pocket expenses;

c. Benefit of the bargain loss; and

d. Punitive damages.

PARTIES

10. Plaintiff Philip Eisen is a California resident who was notified on July 30, 2020 by Planned Parenthood that his personal information had been compromised in the Blackbaud data breach.

11. Defendant Blackbaud, Inc. is a Delaware corporation with its principal place of business located at 65 Fairchild Street, Charleston, South Carolina.

12. Blackbaud is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal

information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.[1]

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1332(d) because this is a class action wherein the amount in controversy exceeds $5,000,000, there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from defendant Blackbaud.

14. This Court has personal jurisdiction over Blackbaud because Blackbaud is registered as "data broker" in California and conducts business in California.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claim occurred in, were directed to, or emanated from this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) and (c)(2) because Blackbaud is subject to the Court's personal jurisdiction in this District.

FACTUAL ALLEGATIONS

A. Blackbaud's Business

16. Blackbaud describes itself as "the world's leading cloud software company powering social good," and claims to have more than 45,000 customers, including nonprofits, foundations, companies, educational institutions, healthcare organizations, and other charitable and nonprofit organizations.

17. Blackbaud has a tailored portfolio of software and services, including solutions for fundraising and CRM, marketing, advocacy, peer-to-peer fundraising, corporate social responsibility, school management, ticketing, grantmaking, financial management, payment processing and analytics.

[1] https://oag.ca.gov/data-broker/registration/185724

18. Blackbaud's cloud solutions are backed by its data intelligence services, which it claims "deliver insights powered by, what we believe is, the world's most robust philanthropic data set." Its specific solutions and services include Blackbaud Raiser's Edge NXT, Blackbaud CRM, Blackbaud eTapestry, Blackbaud TeamRaiser, Blackbaud Peer-to-Peer Fundraising, everydayhero, Blackbaud Guided Fundraising, Blackbaude Volunteer Network Fundraising, Blackbaud Luminate Online, Blackbaud Online Express, Blackbaud Attentive.ly, Blackbaud School Website System, Blackbaud Financial Edge NXT, Blackbaud Tuition Management, Blackbaud Financial Aid Management, Blackbaud Grantmaking, Blackbaud Award Management, Blackbaud Student Information System, Blackbaud Learning Management System, Blackbaud Enrollment Management System, Blackbaud Altru, Blackbaud Church Management, YourCause, Blackbaud Merchant Services, and Blackbaud Purchase Cards.

C. The Data Breach

19. The data breach began on or about February 7, 2020, and according to Blackbaud, was not discovered by Blackbaud until May 14, 2020, when Blackbaud personnel noticed a suspicious log-in on an internal server. According to Blackbaud, all traces of the hacker and its attempt to regain access ceased by June 3.

20. After accessing Blackbaud's system and removing a copy of a "subset of data" from Blackbaud's self-hosted environment, the hacker contacted Blackbaud and demanded ransom to be paid in Bitcoin to destroy the stolen data. On June 18, 2020, the hacker provided Blackbaud with what was purported to be a statement of involved files. A third-party forensic assessor provided an official report to Blackbaud regarding the incident on June 25, 2020, which confirmed the forensic data had been taken. Blackbaud has not disclosed any of the details of that report. Blackbaud ultimately paid the hacker a ransom in an undisclosed amount in Bitcoin.

21. On July 16, 2020, two months after it says it discovered the attack, Blackbaud began notifying its customers of the data breach.

22. Blackbaud's customers have been notified that individual consumers' personal information that they provided to Blackbaud was compromised in the data breach. Reports have indicated that 25,000 organizations were affected. Affected organizations include Harvard University, Emerson College, Boston University, Middlebury College, California Lutheran University, National Public Radio, California State University Northridge, the Archdiocese of Los Angeles, the Boy Scouts of America, the March of Dimes, the American Civil Liberties Union, the American Heart Association, the City University of New York, the University of California at Davis, the University of Texas at Austin, Ambrose University, Auburn University Foundation, Bentley University, Des Moines University, Louisiana Tech University Foundation, Middlebury College, New College of Florida, Rhode Island School of Design, St. Mary's College of Maryland Foundation, Texas Tech Foundation, University of Dayton, University of North Carolina, University of North Florida, Ventura College Foundation, West Virginia University Foundation, and Planned Parenthood. Blackbaud has not released a comprehensive list of those customers affected by the data breach.

23. Blackbaud has since acknowledged that the admitted vulnerability that permitted the data breach to take place was not detected until this incident.

24. Blackbaud has not disclosed any information about the vulnerability that led to the breach. Upon information and belief, Blackbaud did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was collecting and retaining.

25. Blackbaud released a statement following the data breach that described the incident this way:

> "In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent

> forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a 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. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted environment. The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident."[2]

26. Blackbaud services known to have been compromised include at least Blackbaud Altru, Financial Edge NXT, Donor Centrics, and Raiser's Edge NXT.

27. Although Blackbaud claimed the hacker did not access any credit card information, bank account information, medical information, or social security numbers, that appears to be inaccurate.

28. Blackbaud customers, like the University of Detroit Mercy, have notified consumers that their social security numbers were one of the fields that may

[2] https://www.blackbaud.com/securityincident

have been removed by the hacker. In its notice to affected donors, the University of Detroit Mercy wrote: "On July 31, 2020, we determined that the information removed by the threat actor may have contained your full name and Social Security Number."[3]

29. Big Thought also notified customers that "Although Blackbaud has stated that all information was encrypted, a social security number or employer identification number (EIN) may have been accessible to the cybercriminal for a small number of contacts."[4]

30. Northwestern Memorial Healthcare has indicated that the hacker may have accessed financial/payment card information.[5]

31. Northwestern Memorial Healthcare and Northwest Kidney Centers have indicated that the hacker may have accessed medical information, including information about treatment, medial record numbers, dates of service, departments of service, treating physicians, clinical information health conditions, and/or medications.[6]

32. While Blackbaud customers have relied on Blackbaud's assurances that social security numbers and other sensitive information was encrypted, these assurances appear to be incorrect.

33. Upon information and belief, the document ID field in Financial Edge NXT for I9 data was not encrypted, which permitted the hacker to access and

---

[3] https://oag.ca.gov/system/files/9028629.PDF

[4] https://www.bigthought.org/announcements/news-announcements/blackbaud-security-breach-and-how-it-affects-you-your-privacy-and-big-thought/

[5] https://www.hipaajournal.com/56000-northwestern-memorial-healthcare-donors-impacted-by-blackbaud-ransomware-attack/

[6] *Id.*;https://www.nwkidney.org/news/blackbaud-cyber-security-breach-may-impact-some-of-northwest-kidney-centers-donors/

exfiltrate consumers' personal information. This data field included, *inter alia*, social security numbers, driver's license numbers, and passport numbers.[7]

34. Upon information and belief, unencrypted information was also accessed from Raiser's Edge. A Blackbaud article regarding encryption on Raiser's Edge details that unencrypted credit card information can be imported into Raiser's Edge by individual customers.[8]

35. Blackbaud has also acknowledged that prior versions of its products, like Blackbaud CRM, stored unencrypted cardholder data.[9] The data accessed by the hacker contains all data that was available and present as of the date of the cyberattack, which likely includes unencrypted data imported through prior versions of Blackbaud products.

36. Further, upon information and belief, a number of Blackbaud products do not currently support multi-factor authentication, which is a substandard security practice, as most organizations now protect confidential information using multi-factor authentication.[10]

37. Upon information and belief, because many Blackbaud products do not currently support multi-factor authentication, the hacker was able to access consumers' first and last names, combined with their username or email address, as well as passwords or security questions and answers that would permit access to online accounts.

38. A number of organizations have questioned Blackbaud's lack of transparency surrounding the incident.

---

[7] https://buildconsulting.com/learning/blackbaud-cybersecurity-incident-response-options/

[8] https://kb.blackbaud.com/articles/Article/51196

[9] https://www.blackbaud.com/files/support/guides/enterprise/400/padsscrm40sp7.pdf

[10] https://buildconsulting.com/learning/blackbaud-cybersecurity-incident-response-options/

39. On July 24, 2020, the Director of Advancement Services from the University of Missouri wrote: "Am I the only person that thinks blackbaud's response is negligent here? I have called, emailed, chatted and they are refusing to provide the data that was stolen. To me it is unacceptable to put the burden on the client to identify backup records that were part of this. IMO blackbaud was responsible for this and they should take responsibility in identifying the records, not the client."[11]

40. In its notice to consumers, the American Civil Liberties Union wrote: "In all candor, we are frustrated with the lack of information we've received from Blackbaud about this incident thus far. The ACLU is doing everything in our power to ascertain the full nature of the breach, and we are actively investigating the nature of the data that was involved, details of the incident, and Blackbaud's remediation plans. We are also exploring all options to ensure this does not happen again, including revisiting our relationship with Blackbaud."[12]

41. A NPR representative wrote: "I've been disturbed over the past couple years by Blackbaud's repeated use of the word 'subset' as almost a euphemism to hide the extent of a problem, whether it's to describe customers affected by the frequent scheduled and unscheduled outages on their hosted data or software, or the number of customers and amount of data compromised in this specific incident." When they've said 'subset', it usually means affecting what seems less like a 'subset' and more like the entirety of customers hosted in a data center; or, in reference to the "subset' of customer data that was compromised, it is more accurately described as the entirety of your organization's hosted application data as of the backup date. I don't think they are being upfront with their current and potential customers about

[11] https://connect.advserv.org/communities/community-home/digestviewer/viewthread?GroupId=301&MessageKey=a97359ec-57bc-4eb3-9010-fee91400ab4e&CommunityKey=f8ef77b1-79ed-4528-88d7-8866d65196aa&tab=digestviewer

[12] https://www.databreaches.net/blackbaud-believes-your-data-is-safe-from-further-misuse-do-you/

the extent of this incident, and it also seems to be part of a pattern of obfuscation regarding the reliability of their hosting services."[13]

E. Consequences of the Blackbaud Breach

42. The potential consequences of the data breach are substantial. Upon information and belief, the hacker did not, as promised, destroy the data. Plaintiff and Class members face a heightened risk that identify thieves will take out loans, mortgage property, open financial accounts in a their names, open credit cards in a their names, use their information to obtain government benefits, file fraudulent tax returns to obtain tax refunds, obtain driver's licenses or identification cards in their names, gain employment in their names, obtain medical services in their names, or give false information to police during an arrest. Hackers also commonly sell personal information to other criminals to enable them to misuse the information.

43. Unfortunately for Plaintiff and Class members, a person whose personal information has been compromised may not fully experience the effects of the data breach for years to come:

> [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 identify 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.[14]

44. At all relevant times, Blackbaud knew, or reasonably should have known, of the importance of safeguarding customers' personal information and the reasonably foreseeable consequences that would occur if its data systems were

[13] https://connect.advserv.org/communities/community-home/digestviewer/viewthread?GroupId=301&MessageKey=a97359ec-57bc-4eb3-9010-fee91400ab4e&CommunityKey=f8ef77b1-79ed-4528-88d7-8866d65196aa&tab=digestviewer

[14] https://www.gao.gov/new.items/d07737.pdf

breached, including, specifically, the significant costs that would be imposed on consumers as a result of a breach.

45. Consumers also must expend time dealing with the consequences of data breaches, which can include time spent reviewing their accounts compromised by the breach, contacting credit card companies, investigating credit monitoring options and self-monitoring accounts.

46. Additionally, consumers face a significant risk that they will be targeted through sophisticated phishing attacks because of the detail of the information that was compromised.

47. Protections that are necessary to users whose security was hacked include identity theft and credit monitoring, which tends to cost roughly $18 to $30 per month, and identity theft insurance, which ranges from $25 to $60 per year, if not more.

48. In sum, the costs to date of Blackbaud's negligent handling of consumers' information are significant, ranging from intangible loss of privacy to tangible financial harm, both known and unknown. Meanwhile, a user taking reasonable precautions to obtain identity theft and credit monitoring and identity theft insurance would have to spend between $241 and $420 per year.

CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action on behalf of themselves and as a class action under Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of:

All natural persons residing in the United States whose personal information was accessed as a result of the Blackbaud data breach (the "Class").

50. Plaintiff also brings this action on behalf of:

All natural persons residing in California whose personal information was accessed as a result of the Blackbaud data breach. (the "California Subclass").

51. Blackbaud has provided its services to organizations across the nation during the relevant period.

52. The members of the Class are so numerous that joinder of all members is impracticable. While the exact number of class members is unknown to plaintiff at this time and can only be ascertained through appropriate discovery, plaintiff believes there are millions of members of the Class. Absent members of the Class may be identified from records maintained by defendant and may be notified of the pendency of this action by mail, using a form notice similar to that customarily used in consumer class actions.

53. There are questions of law and fact common to the Class, including:

a. Whether Blackbaud's response to the data breach fell below commercially reasonable standards with respect to the protection of that information;

b. Whether Blackbaud implemented and maintained reasonable security procedures and practices appropriate to storing plaintiff's and Class members' personal information;

c. Whether Blackbaud acted negligently in connection with its monitoring and protection of Plaintiff and Class members' personal information;

d. Whether the data breach was made possible by Blackbaud's substandard data security measures and practices;

e. Whether Blackbaud adequately addressed and fixed the vulnerability that permitted the data breach to occur;

f. Whether Plaintiff and other Class members are entitled to credit monitoring and other monetary relief;

g. Whether Blackbaud violated California consumer privacy and unfair competition laws; and

h. The appropriate Class-wide measure of damages.

54. At the time of the data breach, plaintiff and Class members had their personal information stored on Blackbaud's servers. Plaintiff's claim is typical of the claims of the Class, and Plaintiff will fairly and adequately protect the interests of that Class.

55. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

56. Plaintiff is represented by counsel who are competent and experienced in the prosecution of class action litigation.

57. The prosecution of separate actions by individual members of the Class would also create a risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendant.

58. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Individual claims are likely too small to prosecute economically on an individual basis. Prosecution as a class action will eliminate the possibility of repetitious litigation. Treatment as a class action will permit a large number of similarly situated persons to adjudicate their common claims in a single forum simultaneously, efficiently, and without the duplication of effort and expense that numerous individual actions would engender. This class action presents no difficulties in management that would preclude maintenance as a class action.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Negligence

59. Plaintiff, on behalf of himself and the Class, incorporates and re-alleges the preceding paragraphs of the complaint.

60. Blackbaud owed a duty to plaintiff and the Class members to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting and protecting their personal information. This duty included designing, maintaining, monitoring and testing Blackbaud's security systems and protocols to ensure that Class members' personal information was protected; implementing processes that would detect a breach of its security system in a timely manner; timely acting upon

warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and maintaining data security measures consistent with industry standards.

61. Blackbaud had a duty to use reasonable care in safeguarding customers' personal information.

62. Blackbaud had a common law duty to prevent foreseeable harm to others. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

63. Blackbaud had a duty to use reasonable security measures required under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect consumers' personal information.

64. Blackbaud had a special relationship with plaintiff and Class members from being entrusted with their personal information, which provided an independent duty of care. Blackbaud had a duty to use reasonable security measures because it undertook to collect, store and use consumers' personal information.

65. When dealing with its customers that engaged Blackbaud to store consumer data, Blackbaud explicitly recognized those businesses have a duty to protect this information. In its Security Policy, Blackbaud states: "Blackbaud is committed to providing products and services that enable customers to comply with the privacy laws applicable to them. We tirelessly track and interpret pending legislation to ensure that Blackbaud provides the features you need to protect the privacy of your constituents while managing data in a compliant way." It also promises its customers: "[O]ur promise to you is that your Blackbaud solution is

always secure, protected, and reliable" through, *inter alia*, "Robust and continuous Cloud Account/Subscription Governance and control monitoring," "Clear security requirements and reporting on data protection, encryption, and monitoring;" and "Routine vulnerability assessments and DDoS automitigation response."

66. Furthermore, in connection with its Privacy Policy, which it acknowledges applies to its customers, Blackbaud promises: "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."

67. Blackbaud also had a duty to safeguard the personal information of plaintiff and Class members and to promptly notify them of a breach because of state laws and statutes that require Blackbaud to reasonably safeguard sensitive personal information, as alleged herein.

68. Timely notification of the breach was required so that, among other things, plaintiff and Class members could take measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other

financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to try to prevent identify theft.

69. Class members whose information was stored on Blackbaud's servers have an interest in the protection of their personally identifiable information.

70. Blackbaud's security practices fell below commercially reasonable standards with respect to the protection of that information by (a) failing to implement and maintain adequate security practices to safeguard Class members' personal information, (b) failing to detect the data breach in a timely manner, and (c) failing to provide adequate and timely notice of the data breach.

71. Plaintiff and the Class have suffered injury in fact and a loss of money or property in the following ways:

a. They have had their present and future property interest in their personally information diminished;

b. They have been deprived of control over their personal information;

c. They may be required to incur the expense of credit report freezes, credit and identity theft monitoring, and identity theft insurance; and

d. They are at imminent risk of future harm from identity theft.

72. The damages to plaintiff and Class members were a proximate, reasonably foreseeable result of Blackbaud's breach of its duties to safeguard the consumers' personal information it was entrusted to keep.

73. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF

(Violation of South Carolina Data Breach Security Act

S.C. Code. Ann. §§ 39-1-90, *et seq.*)

74. Plaintiff, on behalf of himself and the Class, incorporates and re-alleges the preceding paragraphs of the complaint.

75. Blackbaud is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

76. Plaintiff's and the Class members' personal identifying information includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

77. Blackbaud is required to accurately notify Plaintiff and Class members following discovery or notification of a breach of its data security system if personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

78. Because Blackbaud discovered a breach of its data security system in which personal identifying information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Blackbaud had an obligation to disclose the Blackbaud data breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

79. By failing to disclose the Blackbaud data breach in a timely and accurate manner, Blackbaud violated S.C. Code Ann. § 39-1-90(A). As a direct and proximate result of Blackbaud's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and the Class members suffered damages, as described above.

80. Plaintiff and the Class members seek relief under S.C. Code. Ann. § 39-1-90(G), including actual damages and injunctive relief.

THIRD CLAIM FOR RELIEF

(Violation of South Carolina Unfair Trade Practices Act

S.C. Code. Ann. §§ 39-5-10, *et seq.*)

81. Plaintiff, on behalf of himself and the Class, incorporates and re-alleges the preceding paragraphs of the complaint.

82. Blackbaud is a "person," as defined by S.C. Code Ann. § 39-5-10(a). South Carolina's Unfair Trade Practices Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

83. Blackbaud advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

84. Blackbaud engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' personal information, which was a direct and proximate cause of the Blackbaud data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Blackbaud data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Blackbaud data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of plaintiff 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 and Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that itdid not reasonably or adequately secure plaintiff 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 and Class members' personal information, including duties imposed by the FTC Act.

85. Blackbaud's acts and practices had, and continue to have, the tendency or capacity to deceive.

86. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security measures and ability to protect the confidentiality of consumers' personal information.

87. Blackbaud intended to mislead plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

88. Had Blackbaud disclosed to plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable personal information of millions of consumers, including plaintiff and Class members. Blackbaud accepted the responsibility of maintaining consumer data while keeping the inadequate state of its security controls secret from the public.

89. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity of the personal information in its possession, and the generally accepted professional standards in the cloud computing

industry. Such a duty is also implied by law due to the nature of the relationship between consumers—including plaintiff and the Class—and Blackbaud, because consumers are unable to fully protect their interests with regard to the personal information in Blackbaud's possession, and place trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiff and Class that contradicted these representations.

90. Blackbaud's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Blackbaud's acts and practices offend established public policies that seek to protect consumers' personal information and ensure that entities entrusted with personal information use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45; and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, et seq.

91. Blackbaud's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of the sensitivity of personal information in its possession; and Blackbaud's admitted duty of trustworthiness and care.

92. Blackbaud's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; and such acts or practices impact the public at large, including the Class members.

93. Blackbaud's unfair and deceptive acts or practices have the potential for repetition Blackbaud's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

94. Blackbaud's violations present a continuing risk to plaintiff and Class members as well as to the general public.

95. Blackbaud intended to mislead plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

96. Blackbaud acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and Class members' rights. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter Blackbaud and others from committing similar conduct in the future.

97. As a direct and proximate result of Blackbaud's unfair and deceptive acts or practices, 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 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.

98. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

FOURTH CLAIM FOR RELIEF

(Breach of Contract)

99. Plaintiff, on behalf of himself and the Class, incorporates and re-alleges the preceding paragraphs of the complaint.

100. Blackbaud's Privacy Policy is an agreement between Blackbaud and its customers, who provided consumers' personal information to Blackbaud, including plaintiff and Class members.

101. Plaintiff and Class members are intended third party beneficiaries of the contract between Blackbaud customers and Blackbaud because the Privacy Policy expressly noted that the contract would benefit the individual consumers whose data

was provided to Blackbaud customers. Blackbaud's Security Policy states: "Blackbaud is committed to providing products and services that enable customers to comply with the privacy laws applicable to them. We tirelessly track and interpret pending legislation to ensure that Blackbaud provides the features you need to protect the privacy of your constituents while managing data in a compliant way."

102. Blackbaud's Privacy Policy states, among other things, that Blackbaud "restrict[s] 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."

103. Blackbaud agreed it would "maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website," claiming: "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."

104. In its Security Policy, Blackbaud emphasized: "Your organization's data security is mission-critical, and we take our commitment to protecting it extremely seriously."

105. Blackbaud on the one side and Blackbaud customers on the other formed a contract when Blackbaud customers engaged Blackbaud for the purpose of collecting and storing personal information of consumers. Blackbaud customers fully performed their obligations under the contracts with Blackbaud.

106. Blackbaud breached its agreement with Blackbaud customers by failing to protect consumers' personal information. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) failed

to have appropriate security protocols and measures in place to protect that information, such as adequate internal and external firewalls, physical security, technological security measures, and encryption; (3) disclosed that information to unauthorized third parties; and (4) failed to promptly alert or give notice of the breach.

107. As a direct and proximate result of Blackbaud's breaches of contract, plaintiff and Class members sustained actual losses and damages as described in detail above, and are also entitled to recover nominal damages.

FIFTH CLAIM FOR RELIEF

(Violation of the California Consumer Privacy Act

Cal. Bus. & Prof. Code §§ 1798.100 et seq.)

108. Plaintiff, on behalf of himself and the California Subclass, incorporates and re-alleges the preceding paragraphs of the complaint.

109. Blackbaud violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent plaintiff and the California Subclass members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Blackbaud's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

110. Blackbaud knew or should have known that its data security practices were inadequate to secure California Subclass members' personal information and that its inadequate data security practices gave rise to the risk of a data breach.

111. Blackbaud failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and stored.

112. Blackbaud is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over $25 million.

113. Blackbaud is a business that collects consumers' personal information, as defined by Cal. Civ. Code §§ 1798.100, *et seq*.

114. Plaintiff seeks injunctive relief in the form of an order requiring Blackbaud to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' personal information, requiring Blackbaud to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass members' authorization, along with an explanation of how the data breach occurred.

115. Plaintiff presently seeks only injunctive relief and any other relief the Court may deem proper pursuant to this section. Prior to initiating a claim for statutory damages, Plaintiff served written notice identifying Blackbaud's violations of Cal. Civil Code § 1798.150(a) and demanding the data breach be cured. If within 30 days Blackbaud has not cured, plaintiff will amend this Complaint to seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

SIXTH CLAIM FOR RELIEF

(Violation of California's Customer Records Act

Cal. Civil Code §§ 1798.80, *et seq*.)

116. Plaintiff, on behalf of himself and the California Subclass, incorporates and re-alleges the preceding paragraphs of the complaint.

117. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

118. Blackbaud is a business that owns, maintains, and licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about plaintiff and California Subclass members.

119. Businesses that own or license computerized data that includes personal information, including Social Security numbers, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82. 489.

120. Blackbaud is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82. 490. Plaintiff and California Subclass members' personal information (e.g., Social Security numbers) includes personal information as covered by Cal. Civ. Code § 1798.82.

121. Because Blackbaud knew that plaintiff's and California Subclass members' personal information was acquired by unauthorized persons during the Blackbaud data breach, Blackbaud had an obligation to disclose the Blackbaud data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82. By failing to disclose the Blackbaud data breach in a timely and accurate manner, Blackbaud violated Cal. Civ. Code § 1798.82. As a direct and proximate result of Blackbaud's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, plaintiff and California Subclass members suffered damages, as described above.

122. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

SEVENTH CLAIM FOR RELIEF

(Violation of California's Unfair Competition Law ("UCL"),

Cal. Bus. & Prof. Code §§ 17200, et seq.)

123. Plaintiff, on behalf of himself and the California Subclass, incorporates and re-alleges the preceding paragraphs of the complaint.

124. Blackbaud has engaged in unlawful, unfair and deceptive practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect plaintiff and California Subclass members' personal information, which was a direct and proximate cause of the Blackbaud data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Blackbaud data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of plaintiff and California Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Blackbaud data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of plaintiff and California Subclass members' personal information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of plaintiff and California Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass 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 and California Subclass

members' personal information, including duties imposed by the FTC Act.

125. Plaintiff and the Class have suffered injury in fact and a loss of money or property in the following ways:

a. They have had their present and future property interest in their personally identifiable information diminished;

b. They have been deprived of the exclusive use of their personally identifiable information;

c. They may be required to incur expenses in connection with obtaining credit report freezes, credit and identity theft monitoring, and identity theft insurance; and

d. They are at imminent risk of future harm from identity theft.

126. Blackbaud's actions were unlawful in that they violated the FTC Act, 15 U.S.C. § 45(n) (allowing the FTC to declare unlawful an act or practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition").

127. Blackbaud's actions were also unfair within the meaning of the UCL in that its conduct was substantially injurious to consumers.

128. Blackbaud's actions were also fraudulent in that they represented a standard of care that it knew or should have known to be false.

129. Had Blackbaud disclosed to plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable personal information of millions of consumers, including plaintiff and California Subclass members. Blackbaud accepted the responsibility of maintaining consumer data while keeping the inadequate state of its security controls secret from the public.

130. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity of the personal information in its possession, and the generally accepted professional standards in the cloud computing industry. Such a duty is also implied by law due to the nature of the relationship between consumers—including plaintiff and the and California Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to the personal information in Blackbaud's possession, and place trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of consumers' data stored in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from plaintiff and Class that contradicted these representations.

131. As a direct and proximate result of Blackbaud's unfair and deceptive acts or practices, plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from 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.

132. Plaintiff and California Subclass members are entitled to restitution in the form of the diminished value of the personal information that was entrusted to Blackbaud.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays as follows:

1. That the Court determines that this action may be maintained as a Class action under Fed. R. Civ. P. 23, and that plaintiff be named representative of the Class.

2. That Blackbaud be adjudged to have negligently caused harm to users' personal information under South Carolina law, which was entrusted to its care.

3. That Blackbaud be adjudged to have breached the South Carolina Data Breach Security Act.

4. That Blackbaud be adjudged to have breached the South Carolina Unfair Trade Practices Act.

5. That Blackbaud be adjudged to have breached the contract between Blackbaud customers and Blackbaud under South Carolina law.

6. That Blackbaud be adjudged to have violated California's Consumer Privacy Act.

7. That Blackbaud be adjudged to have violated California's Unfair Competition Law.

8. That judgment be entered for Plaintiff and members of the Class against Defendants for damages and special damages, including any punitive damages allowed by law, together with the costs of this action, including reasonable attorneys' fees.

9. That plaintiff and the Class be awarded pre-judgment and post-judgment interest at the highest legal rate from and after the date of service of this Complaint to the extent provided by law.

10. That plaintiff and members of the Class have such other, further, or different relief, as the case may require and the Court may deem just and proper under the circumstances.

Dated: September 11, 2020

MARC M. SELTZER
KRYSTA KAUBLE PACHMAN
SUSMAN GODFREY L.L.P.

By: */s/ Marc M. Seltzer*
Marc M. Seltzer
Attorneys for Plaintiff Philip Eisen

DEMAND FOR JURY TRIAL

Plaintiff requests a jury trial on all matters so triable.

Dated: September 11, 2020

MARC M. SELTZER
KRYSTA KAUBLE PACHMAN
SUSMAN GODFREY L.L.P.

By: */s/ Marc M. Seltzer*
Marc M. Seltzer
Attorneys for Plaintiff Philip Eisen