ROB BONTA
Attorney General of California
KATHLEEN BOERGERS
Acting Senior Assistant Attorney General
KARLI EISENBERG
Supervising Deputy Attorney General
DARCIE TILLY (SBN 239715)
Deputy Attorney General
600 West Broadway, Suite 1800
San Diego, CA 92101
P.O. Box 85266
San Diego, CA 92186-5266
Telephone: (619) 738-9559
E-mail: Darcie.Tilly@doj.ca.gov

ROB BONTA
Attorney General of California
NICKLAS AKERS
Senior Assistant Attorney General
STACEY SCHESSER
Supervising Deputy Attorney General
YEN P. NGUYEN (SBN 239095)
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3542
E-mail: TiTi.Nguyen@doj.ca.gov

Attorneys for Plaintiff, the People of the State of California

[EXEMPT FROM FILING FEES PURSUANT TO GOVERNMENT CODE SECTION 6103]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN DIEGO

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, v. BLACKBAUD, INC., a corporation, Defendant.	Case No. [PROPOSED] FINAL JUDGMENT AND PERMANENT INJUNCTION

TABLE OF CONTENTS

Plaintiff, the People of the State of California ("Plaintiff" or "Attorney General"), has filed a Complaint for permanent injunction and other relief in this matter, alleging that Defendant Blackbaud, Inc. ("Defendant" or "Blackbaud") violated California Business and Professions Code sections 17200 et seq. and 17500 et seq. Plaintiff, by its counsel, and Defendant, appearing through counsel, have agreed to the entry of this Final Judgment ("Judgment") by the Court without the taking of proof and without trial or adjudication of any fact or law and with all parties having waived their right to appeal. The Court, having considered the matter and good cause appearing, states as follows:

IT IS HEREBY ORDERED, ADJUDGED AND DECREED THAT:

PARTIES AND JURISDICTION

1. The People of the State of California is the Plaintiff in this case.

2. Blackbaud, Inc. is the Defendant in this case. Blackbaud is a Delaware corporation with its principal office located at 65 Fairchild Street, Charleston, South Carolina 29492.

3. This Court has jurisdiction over the allegations and subject matter of the People's Complaint filed in this action, and the parties to this action; venue is proper in this County; and this Court has jurisdiction to enter this Judgment and to enforce its provisions.

4. Jurisdiction is proper because Blackbaud has transacted business within the State of California, and San Diego County, and/or has engaged in conduct impacting the State of California or its residents at all times relevant to the claims at issue.

DEFINITIONS

5. In addition to terms defined elsewhere in the Judgment, for the purposes of this Judgment:

a. "2020 Data Breach" shall mean the Security Incident, first publicly announced by Blackbaud on July 16, 2020, in which a person or persons gained unauthorized access to the Blackbaud Network.

b. Blackbaud shall include Blackbaud and its directors, officers, employees, representatives, agents, affiliates, parents, subsidiaries, predecessors, assigns, and successors.

c. "Blackbaud User" shall mean any employee, representative, contractor, subcontractor or agent of Blackbaud for whom Blackbaud has created a user account and credentials to access the Blackbaud Network.

d. "Blackbaud Customer" shall mean any entity that has contracted with Blackbaud to receive Blackbaud products and/or services and has stored Personal Information and/or Protected Health Information in connection with the use of such products and/or services.

e. "Blackbaud Network" shall mean all networking equipment, technical infrastructure relating to on-prem, cloud-based, and/or colo databases or data stores, applications, servers, and endpoints that: (a) are capable of using and sharing software, data, and hardware resources; (b) are owned, operated, and/or controlled by Blackbaud; and (c) process, store, or have access to Personal Information and/or Protected Health Information of Consumers who reside in the United States.

f. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103.

g. "Clearly and Conspicuously" shall mean that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by Blackbaud Customers, including in all of the following ways:

i. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a video, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made through only one means.

ii. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

iii. An audible disclosure, including by telephone or video, must be delivered in a volume, speed, and cadence sufficient for representatives of Blackbaud Customers to easily hear and understand it.

iv. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable (hard to miss).

v. The disclosure must use understandable language, diction, and syntax. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

vi. The disclosure must be reasonably accessible to Blackbaud Customers with disabilities. For disclosures provided online, this means that Blackbaud may take into account industry standards such as Web Content Accessibility Guidelines, version 2.1 of June 2018, from the World Wide Web Consortium, but nothing in this Judgment precludes Blackbaud from determining on a product-by-product basis how to make information reasonably accessible.

vii. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

h. "Compensating Controls" shall mean alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer or his or her designee to be impractical or unreasonable to implement at the applicable time due to legitimate technical or business constraints. Such alternative mechanisms must: (a) meet the intent and rigor of the original stated requirement; (b) provide a similar level of security as the original stated requirement; (c) be materially and substantively up-to-date with current industry accepted security protocols; and (d) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the Chief Information Security Officer or his or her designee agrees with

both the risk analysis and the determination that the risk is acceptable. Compensating Controls shall not be utilized as permanent alternative security measures and shall be reevaluated for security effectiveness at least every ninety (90) days to determine whether to retain the Compensating Control as the appropriate security measure or to implement an alternative as the permanent security measure. Written security effectiveness documentation shall be prepared and reviewed by the Chief Information Security Officer or his or her designee and shall be kept for a period of one (1) year following the termination of usage of any such alternative mechanism.

i. "Consumer" shall mean any individual whose Personal Information and/or Protected Health Information is processed, stored, or otherwise made accessible on behalf of Blackbaud Customers on the Blackbaud Network. This definition excludes (i) Blackbaud employees, directors, representatives, contractors, subcontractors, agents and their dependents as well as (ii) the business contact information of Blackbaud Customer employees or authorized agents that is stored on Blackbaud corporate systems.

j. "Consumer Protection Laws" shall mean Business and Professions Code section 17200 et seq. and Business and Professions Code section 17500 et seq.

k. "Covered Entity" shall be defined in accordance with 45 C.F.R. § 160.103.

l. "Data Breach Notification Law" shall mean Civil Code § 1798.82.

m. "Effective Date" shall mean the date this Judgment is served on Blackbaud via email to the recipients identified below at paragraph 89, except as otherwise noted in this Judgment.

n. "Encrypt", "Encrypted" or "Encryption" shall mean encoding data into ciphertext—at rest or in transit—rendering it unusable, unreadable, or indecipherable without converting the ciphertext to plaintext, through the use of a reasonable confidential process and key, leveraging a security technology, methodology, or encryption algorithm commensurate with the sensitivity of the data at issue.

o. "Governance Process" shall mean any written policy, standard, procedure, or process (or any combination thereof) designed to achieve a control objective with respect to the Blackbaud Network.

p. "HIPAA" shall mean the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226.

q. "Personal Information" or "PI" shall mean information regarding a Consumer residing in California that falls within one of the following categories:

i. A first name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (i) Social Security number; (ii) driver's license number; (iii) state- or federally-issued identification card number; or (iv) financial account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the consumer's financial account;

ii. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical characteristics or digital representation thereof;

iii. A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account; or

iv. Any category of personal information found in the definition set forth in the Data Breach Notification Law and Personal Information Protection Law.

r. "Personal Information Protection Law" shall mean Civil Code section 1798.81.5.

s. "Protected Health Information" or "PHI" shall mean the Protected Health Information or PHI, as defined in accordance with 45 C.F.R. § 160.103, of a Consumer.

t. "Security Incident" shall mean any compromise, or imminent threat of a compromise to the confidentiality, integrity, or availability of PI or PHI stored within, accessed, or transmitted through the Blackbaud Network, by unauthorized access or inadvertent disclosure, including but not limited to an incident for which notification may be required under the Data Breach Notification Law or HIPAA. For purposes of this definition, "availability" shall not

include an intentional limitation on the availability of PI or PHI, such as for purposes of performing maintenance on the Blackbaud Network.

INJUNCTION

6. Pursuant to California Business and Professions Code sections 17203 and 17535, as of the Effective Date, Blackbaud shall engage in or refrain from engaging in the practices as identified in this Judgment.

7. The duties, responsibilities, burdens, and obligations undertaken in connection with this Judgment apply to Blackbaud.

I. COMPLIANCE WITH THE LAW

8. Blackbaud shall comply with the Consumer Protection Law and Personal Information Protection Law in connection with its processing, storing and safeguarding of PI and/or PHI.

9. Blackbaud shall comply with the Data Breach Notification Law, as applicable.

10. Blackbaud shall comply with HIPAA, as applicable, including the Privacy Rule (45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E) and Security Rule (45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C), and shall implement all Administrative, Technical, and Physical Safeguards required by HIPAA. "Administrative Safeguards", "Technical Safeguards" and "Physical Safeguards" shall be defined in accordance with 45 C.F.R. §§ 164.304, 164.308, 164.310, 164.312.

11. Blackbaud shall not make a misrepresentation which is capable of misleading Blackbaud Customers or Consumers, or fail to state a material fact if that failure is capable of misleading Blackbaud Customers or Consumers, regarding the extent to which Blackbaud maintains and/or protects the privacy, security, confidentiality, or integrity of PI or PHI of Consumers.

12. Blackbaud shall not make a misrepresentation which is capable of misleading Blackbaud Customers or Consumers, or fail to state a material fact if that failure is capable of misleading Blackbaud Customers or Consumers, regarding the likelihood that PI or PHI affected by a Security Incident may be subject to further unauthorized access, disclosure or other misuse.

13. Blackbaud shall not misrepresent to Blackbaud Customers the notification requirements of the Data Breach Notification Law or HIPAA.

II. SECURITY INCIDENT RESPONSE AND SECURITY INCIDENT RESPONSE PLAN

14. Blackbaud shall implement and maintain written incident response plan(s) to prepare for and respond to Security Incidents ("Incident Response Plan").

15. Such a plan shall, at a minimum, identify and describe the following phases:

a. Preparation;

b. Detection and Analysis;

c. Containment;

d. Eradication;

e. Recovery; and

f. Post-Incident Analysis and Remediation.

16. Blackbaud shall investigate Security Incidents. Blackbaud shall maintain documentation sufficient to show the investigative and responsive actions taken in connection with each Security Incident and the determination as to whether notification under the Data Breach Notification Law or HIPAA is required. Blackbaud shall also assess whether there are reasonably feasible training or technical measures, in addition to those already in place, that would materially decrease the risk of the same type of Security Incident from reoccurring. Blackbaud shall revise and update the Incident Response Plan, as necessary, to adapt to any changes to the Blackbaud Network.

17. Blackbaud shall conduct, at a minimum, exercises ("table-top exercises") twice a year to test and assess its preparedness to respond to a Security Incident.

III. BREACH RESPONSE AND NOTIFICATION

18. Blackbaud shall implement and maintain a Breach (as defined below) response plan that contains policies and procedures for (a) notification and coordination with law enforcement, as appropriate, and Blackbaud Customers; (b) affected Blackbaud Customer response (including consideration of appropriate staffing levels, training, and written materials); and (c) regulator notification, as applicable.

19. In the case that a Security Incident requires notification under the Data Breach Notification Law or HIPAA ("Breach"), Blackbaud shall do the following:

a. Blackbaud shall timely notify affected Blackbaud Customers in accordance with the Data Breach Notification Law, HIPAA, and any applicable contracts with Blackbaud Customers.

b. Consistent with Blackbaud's obligations set forth in Paragraphs 20 and 19.c, Blackbaud shall Clearly and Conspicuously provide affected Blackbaud Customers with such information that each Blackbaud Customer requires to provide timely notice to affected Consumers and the Plaintiff in accordance with the Data Breach Notification Law and HIPAA, as applicable.

c. To the extent possible and consistent with the mutually agreed roles and responsibilities under the applicable contract between Blackbaud and a Blackbaud Customer, if the identity of affected Consumers cannot be determined by a Blackbaud Customer following Blackbaud's provision of the guidance and/or assistance set forth in Paragraph 20 of this Judgment, Blackbaud shall assist Blackbaud Customers in determining the names of affected Consumers in such Blackbaud Customer's affected databases.

20. In determining whether notification to Blackbaud Customers under the Data Breach Notification Law or HIPAA is required, Blackbaud shall consider information stored by affected Blackbaud Customers, including information stored in fields not intended for PI and/or PHI in the affected Blackbaud products. Blackbaud shall also offer Blackbaud Customers reasonable guidance, cooperation and/or assistance, including with respect to instructions on how to run queries and reports of Blackbaud Customer databases affected by the Security Incident so that Blackbaud Customers can determine whether they must provide notification to Consumers in time to allow such notification in accordance with the Data Breach Notification Law or HIPAA. If after a Blackbaud Customer has sought and received such guidance, cooperation and/or assistance, the Blackbaud Customer is unable to run such queries and reports itself, Blackbaud shall reasonably run such queries and reports for the Blackbaud Customers at no cost, if requested by the Blackbaud Customer.

21. Blackbaud shall specify in any new contracts entered into with Blackbaud Customers after the Effective Date the roles and responsibilities to be undertaken by Blackbaud and the Blackbaud Customer in the event of a Breach, specifically for providing notice to affected Consumers and the Attorney General, as required by the Data Breach Notification Law or HIPAA, as appropriate.

22. If Blackbaud determines that a Security Incident does not require notification under the Data Breach Notification Law or HIPAA, Blackbaud shall create documentation that includes a description of the Security Incident and Blackbaud's response to that Security Incident ("Security Incident Report"). Blackbaud shall make any Security Incident Report available to the Attorney General upon written request.

23. Blackbaud shall conduct, at a minimum, exercises ("table-top exercises") twice a year to test and assess its preparedness to respond to a Breach. These exercises shall include the following, as appropriate:

a. Planning for sufficient staffing levels to handle a high volume of questions from affected Blackbaud Customers and to provide Blackbaud Customers with information in a reasonable amount of time;

b. Planning employee training to provide relevant, useful, and accurate information to Blackbaud Customers;

c. Preparing written materials to provide to Blackbaud Customers that Clearly and Conspicuously disclose relevant information.

IV. INFORMATION SECURITY PROGRAM

24. Unless otherwise specified herein, within thirty (30) days after the Effective Date, Blackbaud shall implement, maintain, periodically review and revise, and comply with a comprehensive information security program ("Information Security Program"), the purpose of which shall be to take reasonable steps to protect the confidentiality, integrity, and availability of PI and PHI on the Blackbaud Network. Blackbaud's Information Security Program shall be documented in the Governance Processes and shall contain administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of Blackbaud's operations;

b. The nature and scope of Blackbaud's activities; and

c. The sensitivity of the PI and PHI on the Blackbaud Network.

25. The Information Security Program required by this Judgment shall include the requirements of Paragraphs 28 through 70 in this Judgment.

26. Should Blackbaud acquire any other entity and/or product, Blackbaud shall perform cybersecurity due diligence to assess such entity's/product's compliance with this Judgment. Blackbaud shall evaluate the requirements that must be met before the entity and/or product is integrated into the Blackbaud Network, including an assessment of whether the entity and/or product meets the requirements of this Judgment and all deficiencies requiring remediation, and Blackbaud shall develop an integration plan reflecting this analysis. After Blackbaud has assured itself of such entity's/product's compliance, and not later than two (2) years after the closing of such acquisition, the acquired entity/product shall be incorporated into the Information Security Program herein. Blackbaud shall document the cybersecurity due diligence required by this Paragraph for each acquisition, which shall be provided to the Attorney General upon request.

27. Blackbaud may satisfy the requirements to implement and maintain an Information Security Program, including but not limited to the written incident response plan and other specific information security requirements, through review, maintenance, and as necessary, updating of Blackbaud's existing information security program and related safeguards, provided that such program and safeguards meet the requirements of this Judgment.

28. Blackbaud shall implement appropriate access controls, including without limitation, least privilege access to only allow authorized users access to necessary resources on the Blackbaud Network for the organization's business needs, consistent with NIST Special Publication 800-53 (page 36-39, AC-6), and zero-trust architecture, consistent with NIST Special Publication 800-207, where technically feasible and commercially reasonable.

29. Blackbaud shall reasonably oversee its third-party vendors who have access to the Blackbaud Network or who hold or store PI or PHI on Blackbaud's behalf by maintaining and

periodically reviewing and revising, as needed, a Governance Process for assessing vendor compliance in accordance with Blackbaud's Information Security Program including whether the vendor's security safeguards are appropriate for that business. That Governance Process shall require vendors in contracts entered into or renewed beginning thirty (30) days after the Effective Date to implement and maintain appropriate safeguards, and further require Blackbaud to make commercially reasonable efforts to require vendors to notify Blackbaud within seventy-two (72) hours of discovering any security incident that may give rise to a Breach (a "Third-Party Reported Incident"). At a minimum, the Governance Process shall require vendors in contracts entered into or renewed beginning thirty (30) days after the Effective Date to notify Blackbaud within five (5) business days of discovering any Third-Party Reported Incident.

30. Blackbaud shall employ an individual who shall be responsible for implementation of Blackbaud Governance Processes relating to compliance with privacy laws, including the Data Breach Notification Law, Personal Information Protection Law, and HIPAA (hereinafter referred to as the "Chief Privacy Officer"). The Chief Privacy Officer shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role, and possess a fundamental understanding of state and federal privacy and data security laws;

b. Assist Blackbaud in complying with Data Breach Notification Law, Personal Information Protection Law, and HIPAA; matters related to Blackbaud's privacy compliance assessments; and coordination with Blackbaud executives and officers as it relates to business operations affecting the privacy, confidentiality, integrity, and security of PI and PHI in the Blackbaud Network; and

c. Provide reports as necessary to the Office of General Counsel, which shall provide reports as necessary to the Chief Executive Officer, and as necessary, to the Board of Directors.

31. Blackbaud shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (hereinafter

referred to as the "Chief Information Security Officer"). The Chief Information Security Officer shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role in implementing, maintaining, and monitoring the Information Security Program;

b. Provide an annual report to the Blackbaud Board of Directors on the adequacy of Blackbaud's Information Security Program;

c. At any meeting of the Board of Directors concerning the security posture or security risks faced by Blackbaud, provide reports to Blackbaud's Board of Directors, and shall inform, advise, and update the Board of Directors regarding Blackbaud's security posture and the security risks faced by Blackbaud; and

d. Notify the Chief Executive Officer of any Security Incident or Third-Party Reported Incident involving over ten (10) Blackbaud Customers within forty- eight (48) hours of discovery, as well as notify a member of Blackbaud's Board of Directors, in the event that the Chief Executive Officer is not a member of the Board of Directors within seventy-two (72) hours of discovery.

32. Blackbaud shall employ one or more individuals to serve as liaison between areas of Blackbaud business and the office of the Chief Information Security Officer regarding implementation, maintenance, and monitoring of the Information Security Program for the area of Blackbaud business (hereinafter referred to as a "Business Information Security Officer"). Each Business Information Security Officer shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of the Business Information Security Officer's role in implementing, maintaining and monitoring the Information Security Program; and

b. Be responsible for regularly informing, advising, and updating the Chief Information Security Officer or his or her designee regarding the security posture of the areas of Blackbaud business for which he or she is responsible for liaising; the security risks faced by the relevant area of Blackbaud business; and the implications of any decision the Business

Information Security Officer makes that may materially impact the security posture of the area of Blackbaud business.

33. Blackbaud shall employ one or more individuals who shall be responsible for developing, maintaining, and monitoring the information technology needs and requirements of Blackbaud's staff, operations, network, and devices (hereinafter may be referred to as the "Chief Technology Officer"). Such individuals shall:

a. Have the education, qualifications, and experience appropriate to the level, size, and complexity of his or her role in developing, maintaining, and monitoring the information technology needs and requirements of Blackbaud's staff, operations, network, and devices;

b. Develop and execute the company's strategy for utilizing technological resources, with the goal of ensuring that all Blackbaud technological resources are up-to-date and patched accordingly, and supervise the Patch Supervisor; and

c. Provide reports as necessary to the Chief Executive Officer and coordinate with the Chief Privacy Officer and Cybersecurity Counsel and Chief Information Security Officer, to take steps to ensure Blackbaud's information technology, information security, and privacy programs are cohesive and aligned.

34. Blackbaud shall provide the Chief Privacy Officer, Chief Information Security Officer, Business Information Security Officers, Chief Technology Officer, Information Security Program and corresponding cybersecurity staff with the resources and support reasonably necessary so that the Information Security Program functions as required by this Judgment.

35. Without limiting the foregoing, Blackbaud may fulfill the specified governance roles and responsibilities in this Judgment with individuals with titles that do not directly correspond to the defined terms in this Judgment; provided that Blackbaud meets the functional requirements of Paragraphs 30-34.

V. TRAINING REQUIREMENTS

36. Employees who are responsible for implementing, maintaining, or monitoring the Information Security Program, including but not limited to the Chief Information Security Officer and Business Information Security Officers, shall receive specialized training to help effectuate

Blackbaud's compliance with the terms of this Judgment. Blackbaud shall provide the training required under this Paragraph to all such employees within thirty (30) days of the Effective Date of this Judgment or prior to an employee starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program. Blackbaud shall document the trainings, including the date(s) upon which they were provided and to whom.

37. Blackbaud shall provide training on safeguarding and protecting PI and PHI to its employees who handle PI or PHI, and its employees responsible for implementing, maintaining, or monitoring the Information Security Program. Such training shall be appropriate to employees' job responsibilities and functions and shall occur on an annual basis, or more frequently if appropriate, beginning within thirty (30) days of the Effective Date of this Judgment or prior to an employee handling PI or PHI or starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program. Blackbaud shall document the trainings, including the date(s) upon which they were provided and to whom.

38. Blackbaud shall provide specialized technology and cybersecurity training, ongoing education, and product training to relevant information technology and information security personnel.

VI. PERSONAL AND PROTECTED HEALTH INFORMATION SAFEGUARDS AND CONTROLS

39. Blackbaud shall maintain and comply with a Governance Process establishing that Blackbaud Customer database backup files containing PI and PHI will be stored to the minimum extent necessary to accomplish Blackbaud's intended legitimate business purpose(s) in storing the information in such database backup files on behalf of Blackbaud Customers. With respect to PHI, the Governance Process shall be consistent with the Minimum Necessary Standard, which shall refer to the requirements of the Privacy Rule that, when using, disclosing, or requesting PHI, a Covered Entity or Business Associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).

40. Blackbaud shall maintain, regularly review and revise as necessary, and comply with a Governance Process to appropriately protect PI and PHI from unauthorized access whether

the information is transmitted electronically from the Blackbaud Network or stored in the Blackbaud Network. Any such Governance Process shall include at a minimum, total database encryption of all databases that contain Blackbaud Customer data. Where appropriate, and until total database encryption of all databases is completed, field-level encryption of data fields that may include PI, PHI, and/or user account credentials on Blackbaud's computer networks shall continue. Blackbaud shall also require all third-party data storage or cloud providers to apply equal to or greater encryption protocols to any Blackbaud Network data.

41. Blackbaud shall maintain, regularly review and revise as necessary, and comply with a Governance Process that provides for the secure disposal, on a periodic basis, of Blackbaud Customer database backup files within Blackbaud's control in accordance with written retention schedules.

42. Blackbaud shall invest in and utilize a solution for searching, monitoring, and tracking the dark web for Blackbaud Network data, including Blackbaud Customer data if there is a Breach. If Blackbaud Network data or a threat to Blackbaud Network data is discovered on the dark web, Blackbaud shall notify the Chief Privacy Officer and Chief Information Security Officer, who shall then notify the Office of General Counsel and Chief Executive Officer, and if applicable, any Blackbaud Customers whose data may be affected.

VII. SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

A. Network Segmentation

43. Blackbaud shall maintain, regularly review and revise as necessary, and comply with network segmentation protocols and related policies that are reasonably designed to properly segment the Blackbaud Network or otherwise implement Compensating Controls, which shall, at a minimum, comply with NIST CSF controls related to network segmentation.

44. Blackbaud shall regularly evaluate, and, as appropriate, restrict and/or disable any unnecessary ports on the Blackbaud Network.

45. Blackbaud shall logically separate its development, production and non-production environments in the Blackbaud Network.

46. Blackbaud shall employ microsegmentation and/or access control security principles in the Blackbaud Network at the following levels: (1) application; (2) database; (3) and user. The requirements of this Paragraph shall commence upon sixty (60) days after the Effective Date.

B. Risk Assessment

47. Blackbaud shall maintain and regularly review and revise as necessary a risk-assessment program designed to identify and assess risks to the Blackbaud Network. Risk assessments shall follow the NIST Cybersecurity Framework, or where required and deemed appropriate, another established industry standard cybersecurity framework and be performed annually under the direction of the Chief Information Security Officer and Blackbaud's General Counsel and shall be documented. In cases where Blackbaud deems a risk to be acceptable, Blackbaud shall generate and retain for at least seven (7) years a record stating why Blackbaud deems the risk to be acceptable and demonstrating how such risk is to be managed in consideration of cost or difficulty in implementing effective countermeasures. All reports shall be maintained by the Chief Information Security Officer or his or her designee and be available for inspection by the Third-Party Assessor described in Paragraph 71 of this Judgment when the Third-Party Assessor is conducting its Third-Party Assessments.

C. Penetration and Security Testing

48. Within sixty (60) days of the Effective Date, Blackbaud shall implement and maintain a risk-based security-testing program reasonably designed to identify, assess, and remediate security vulnerabilities within the Blackbaud Network. This program shall include: (i) testing for security vulnerabilities for Blackbaud developed applications before deployment to any public-facing webserver using static and dynamic application testing for production releases; (ii) at least one annual penetration test of all Blackbaud products; (iii) vulnerability scans of all systems in the Blackbaud Network occurring at least weekly; and (iv) vulnerability scans of the production environment of the Blackbaud Network within twenty-four (24) hours after any material modifications. All results shall be documented and maintained for two (2) years.

49. Blackbaud shall rate and rank the criticality of all vulnerabilities identified as a result of any vulnerability scanning or penetration testing that it performs on the Blackbaud Network in alignment with an established industry-standard framework (e.g., NVD, CVSS, or equivalent standard). For each vulnerability that is ranked as most critical, Blackbaud shall commence remediation planning within seventy-two (72) hours after the identification of the vulnerability and shall apply the remediation within fifteen (15) days after the identification of the vulnerability. If the remediation cannot be applied within fifteen (15) days after the identification of the vulnerability, Blackbaud shall identify existing or implement new Compensating Controls designed to protect PI and PHI as soon as practicable but no later than fifteen (15) days after the identification of the vulnerability. All results shall be documented and maintained for three (3) years.

D. Access Control and Account Management

50. Blackbaud shall implement and maintain appropriate controls to manage access to, and use of, all Blackbaud User accounts with access to Blackbaud Customer databases that store Consumer data, including, without limitation, individual accounts, administrator accounts, service accounts, and vendor accounts.

51. To the extent that Blackbaud maintains accounts requiring passwords:

a. Such controls shall be consistent with the requirements of NIST or another established industry standard cybersecurity framework, including reasonable password confidentiality and password-rotation policies; or multi-factor authentication, tokens, or any other equal or greater authentication protocol. For purposes of this Paragraph, any administrative-level passwords shall be Encrypted or secured using a reasonable password vault, privilege access monitoring, or other Compensating Control; and

b. Blackbaud shall implement and maintain appropriate policies for the secure storage of Blackbaud Network account passwords based on industry accepted security practices; for example, hashing and salting passwords stored online using an appropriate hashing algorithm that is not vulnerable to a collision attack together with an appropriate salting policy, or other equivalent or stronger protections.

52. Blackbaud shall implement and maintain appropriate access controls, processes, and procedures, the purpose of which shall be to grant access to the Blackbaud Network only after the Blackbaud User, or Blackbaud Customer user, as applicable, has been properly identified and authenticated.

53. For Blackbaud Users that are employees or independent contractors of Blackbaud, Blackbaud shall as soon as practicable and (i) within one (1) business day of the termination of the Blackbaud User's employment or contract with Blackbaud for Privileged Accounts, or (ii) within three (3) business days of the termination of the Blackbaud User's employment or contract with Blackbaud for standard accounts, terminate access for all such terminated Blackbaud Users. Blackbaud User accounts issued to a third party will be set to automatically expire whenever technically feasible for a period not to exceed one hundred and eighty (180) days from when the account was created. For purposes of this subsection, the date of termination shall be the date recorded by Blackbaud's Human Resources Department. "Privileged Accounts" shall mean accounts that provide the ability to make system and software configuration changes, perform administrative tasks, and create or modify Blackbaud User accounts. All access terminations shall be documented and maintained for five (5) years.

54. Blackbaud shall limit the access of Blackbaud Users to Blackbaud Customer databases that store Consumer data on a least-privileged basis.

55. Blackbaud shall regularly inventory the Blackbaud Users who have access to the Blackbaud Network in order to review and determine whether or not such access remains necessary or appropriate. Blackbaud shall compare termination lists to Blackbaud User accounts to determine whether access privileges have been appropriately terminated. At a minimum, such review shall compare termination lists to Blackbaud User accounts to determine whether access privileges have been appropriately terminated on a quarterly basis. The requirements of this subsection shall commence upon sixty (60) days after the Effective Date.

56. Within sixty (60) days of the Effective Date, Blackbaud shall implement Privileged Access Management administration processes and procedures to store and monitor the account credentials and access privileges of Blackbaud Users who have Privileged Accounts,

administrator accounts, and/or accounts, active or available, to design, maintain, operate, and update the Blackbaud Network.

57. Blackbaud shall implement and maintain controls to detect anomalous activity by unauthorized devices and prevent unauthorized devices from accessing the Blackbaud Network.

E. File Integrity Monitoring

58. Blackbaud shall maintain controls designed to provide near real-time notification of unauthorized or malicious modifications to Blackbaud Customer database servers in the Blackbaud Network. The notification shall include information available about the modification including, where available, the date of the modification, the source of the modification, the type of modification, and the method used to make the modification.

F. Unauthorized or Malicious Applications

59. Blackbaud shall maintain controls designed to identify and protect against the execution or installation of unauthorized or malicious applications on the Blackbaud Network.

G. Logging and Monitoring

60. Within sixty (60) days of the Effective Date, Blackbaud shall implement reasonable controls to centralize monitoring, logging, and operational activities on the Blackbaud Network; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance.

61. All Security Incidents shall promptly be reported to the Chief Information Security Officer and the Office of the Chief Privacy Officer consistent with the timeframes specified in the Blackbaud Incident Response Plan which, to the extent applicable, shall be aligned to NIST 800-61r2 and include processes for communicating Security Incidents to the appropriate leaders, executives, and committees to appropriately manage the risk. Any critical vulnerability that is associated with a Security Incident shall be remediated within twenty-four (24) hours of the identification of such vulnerability. If that vulnerability cannot be remediated as indicated above, then Blackbaud shall within twenty-four (24) hours of the identification of such vulnerability: (a) implement Compensating Controls; or (b) take the application or functionality of the application

affected by such vulnerability offline until such vulnerability is remediated or Compensating Controls have been successfully applied.

62. Blackbaud shall monitor on a daily basis, and shall test on at least a monthly basis, any tool used to monitor the Blackbaud Network for the occurrence of a Security Incident, and properly configure, regularly update, and maintain the tool, so that the Blackbaud Network is appropriately monitored.

H. Change Control

63. Blackbaud shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to manage and document changes to the Blackbaud Network. At a minimum:

a. Blackbaud shall define the roles and responsibilities for those involved in the change control process, including a board responsible for reviewing changes (hereinafter referred to as the "Change Advisory Board"). The Change Advisory Board shall include stakeholders from the appropriate business and informational technology units. The Change Advisory Board's responsibilities shall include: managing overall change control policies and procedures; providing guidance regarding the overall change control policies and procedures; conducting an annual audit of change requests so that changes to the Blackbaud Network are properly analyzed and prioritized; and reviewing, approving, evaluating, and scheduling requests for changes to the Blackbaud Network.

b. The change control policies and procedures shall address the process to: request a change to the Blackbaud Network; determine the priority of the change; determine the change's impact on the Blackbaud Network, the security of PI and PHI on the Blackbaud Network, and Blackbaud's ongoing business operations; obtain the appropriate approvals from required personnel (e.g., change requester, area of Blackbaud business, Change Advisory Board); develop, test, and implement the change; and review and test the impact of the change on the security of the Blackbaud Network, in each case as appropriate, based on the risk.

c. The change control policies and procedures required by this Paragraph shall require that any architectural changes to the Blackbaud Network be evaluated regarding

potential risks, and that all such changes receive appropriate (i) analysis, (ii) approvals from required personnel, and (iii) testing, as appropriate, based on the risk.

d. Any action with respect to any changes to the Blackbaud Network (requesting, analyzing, approving, developing, implementing, and reviewing) shall be documented and retained, with the documentation appropriately secured and stored in repositories that are scoped to an application, area of Blackbaud business, and/or geography and are accessible to appropriate security personnel.

I. Asset Inventory

64. Blackbaud shall utilize processes and, where practicable, automated tool(s) to regularly inventory and classify, and issue reports on, all assets that comprise the Blackbaud Network. The asset inventory as well as applicable configuration and change management systems shall, at a minimum, collectively identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the Blackbaud Network; (e) the asset's criticality rating; (f) the potential risks and vulnerabilities associated with each asset; and (g) whether the asset processes or stores PI or PHI of Consumers. For purposes of this Paragraph, "assets" shall mean network components, data stores, physical devices, systems, software platforms, and applications within the Blackbaud Network. The requirements of this Paragraph shall commence upon sixty (60) days after the Effective Date.

J. Digital Certificates

65. Blackbaud shall implement and maintain a Governance Process to manage the life cycle of all digital certificates that expire longer than a week after their creation and that are used to authenticate servers and systems in the Blackbaud Network, including whether to issue, cancel, renew, reissue, or revoke a digital certificate. The Governance Process required by this Paragraph shall track the expiration date of any such digital certificate and require notification of such expiration to the custodian of the certificate key thirty days (30) prior to expiration, ten days (10) prior to expiration, and on the date the digital certificate expires. Digital certificate for purposes of this Paragraph shall include a security token, biometric identifier, or a cryptographic key used to protect externally-facing systems and applications.

K. Endpoint Detection and Response ("EDR")

66. Blackbaud shall acquire, configure, and utilize, an EDR solution to incorporate real-time threat detection and analysis across the Blackbaud Network and Blackbaud owned and/or managed devices. Blackbaud shall operationally staff and manage such EDR solution with the necessary and qualified information security personnel and analyst technicians needed to operate and manage the solution. In addition to any in-house information security personnel and analyst technicians, Blackbaud shall also retain as part of any solution configuration, EDR solution professional services to assist with near real- time threat detection and monitoring.

L. Intrusion Detection and Prevention Tools

67. Blackbaud shall implement, maintain, and update intrusion detection and prevention tools including but not limited to host-based firewalls, antivirus/antimalware software, and logging on all internal servers and employee computers on the Blackbaud Network to detect and prevent malicious activity.

M. Threat Management

68. Blackbaud shall establish a threat management program which shall include the use of automated tools to continuously monitor the Blackbaud Network for active threats. Blackbaud shall continuously monitor, and assess on at least a monthly basis, whether any monitoring tool used pursuant to this Paragraph is appropriately configured, tested, and updated.

N. Updates and Patch Management

69. Within sixty (60) days of the Effective Date, Blackbaud shall maintain, keep updated, and support the software on the Blackbaud Network, taking into consideration the impact a software update will have on data security in the context of the Blackbaud Network and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. At a minimum, Blackbaud shall also do the following:

a. For any software that will no longer be supported by its manufacturer or a third party, Blackbaud shall commence the evaluation and planning to replace the software or to maintain the software with appropriate Compensating Controls the later of one (1) year prior to the date on which the manufacturer's or third party's support will cease, or ninety (90) days from

the date the manufacturer or third party announces that it is no longer supporting the software if such period is less than one (1) year. If Blackbaud is unable to commence the evaluation and planning in the timeframe required by this subparagraph, it shall prepare and maintain a written exception that shall include:

i. A description of why the exception is appropriate, e.g., what business need or circumstance supports the exception;

ii. An assessment of the potential risk posed by the exception; and

iii. A description of the schedule that will be used to evaluate and plan for the replacement of the software or addition of any Compensating Controls.

b. Blackbaud shall maintain reasonable controls to address the potential impact security updates and security patches may have on the Blackbaud Network and shall:

i. Maintain a patch management solution(s) to manage software patches that includes the use of standardized patch management distribution tool(s), including automation-assisted processes, whenever appropriate; and

ii. Maintain a tool that includes an automated Common Vulnerabilities and Exposures ("CVE") feed. The CVE tool required by this subparagraph shall provide Blackbaud regular updates, including daily updates to the extent available, regarding known CVEs for vendor-purchased software applications in use within the Blackbaud Network. Blackbaud may satisfy its obligations under this subparagraph by using an industry-standard vulnerability scanning tool. The CVE tool required by this subparagraph shall also:

1. Identify, confirm, and enhance discovery of the parts of the Blackbaud Network that may be subject to CVE events and/or incidents;

2. Scan the Blackbaud Network for CVEs; and

3. Scan the Blackbaud Network to determine whether scheduled security updates and patches have been successfully installed, including whether any security updates or patches rated as critical have been installed consistent with the requirement of this Judgment.

c. Blackbaud shall appoint one or more individuals responsible for patch management relating to the Blackbaud Network ("Patch Management Group") Blackbaud shall appoint one or more individuals who shall be responsible for overseeing the Patch Management Group ("Patch Supervisor"). The Patch Supervisor and the members of the Patch Management Group shall include persons with appropriate experience and qualifications. The Patch Management Group shall be responsible for:

i. Monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from the tools installed pursuant to subparagraph (69.b) and completing appropriate and timely application of all relevant security updates and/or security patches;

ii. Monitoring compliance with policies and procedures regarding ownership, supervision, evaluation, and coordination of the maintenance, management, and application of all security patches and software and application security updates by appropriate information technology (IT) application and system owners;

iii. Supervising, evaluating, and coordinating any system patch management tool(s) such as those identified in subparagraph (69.b); and

iv. A training requirement for individuals responsible for implementing and maintaining Blackbaud's patch management policies.

d. Blackbaud shall use the inventory created pursuant to Paragraph 64 in its regular operations to assist in identifying assets within the Blackbaud Network for purposes of applying security updates or security patches that have been released.

e. Blackbaud shall employ processes, procedures, and technology for the timely scheduling and installation of any security update and security patch relevant to the Blackbaud Network. Security update and security patch scheduling and installation shall be based upon priority of threat level, services storing PI and/or PHI, and public/external facing services that are processing PI and/or PHI. Blackbaud shall also consider NIST SP 800-40r4 ("Guide to Enterprise Patch Management Planning") and any relevant severity ratings, security alerts, and advisory notices disseminated by software and application vendors, the Cybersecurity and

Infrastructure Security Agency (CISA), and/or an equivalent United States Department of Homeland Security (DHS) agency designated as responsible for cybersecurity. Blackbaud may adjust the severity rating of the security update or security patch using a risk-based approach that is documented with written explanation. If Blackbaud is unable to schedule and install the security update or security patch in accordance with the applicable severity or risk-based rating, Blackbaud shall identify the assets to which it applies, and create a written explanation that shall include:

i. A description of why the action is appropriate, e.g., what business need or circumstance exists that supports the rating;

ii. A description of the alternatives that were considered, and why they were not appropriate;

iii. An assessment of the potential risks posed by the action;

iv. The anticipated length of time for the action, if the action is temporary; and

v. To the extent applicable, a plan for managing or mitigating those risks identified in subparagraph (69.e.iii) (e.g., Compensating Controls, alternative approaches, methods). The written explanation required by this subparagraph shall be prepared within forty-eight (48) hours of its determination to apply an exception.

f. Blackbaud shall, within a time period appropriate to the risk to the Blackbaud Network, but not later than forty-eight (48) hours of rating any security update or patch as critical or critical zero-day, either: (1) apply such update or patch to the Blackbaud Network; (2) apply Compensating Controls; or (3) if Blackbaud is unable to timely update or patch the Blackbaud Network, or apply Compensating Controls, Blackbaud will take the identified application or affected functionality of the identified application offline until the update or patch or Compensating Controls has been successfully applied. If Blackbaud chooses not to apply such update or patch to the Blackbaud Network and instead to implement Compensating Controls, it shall prepare and maintain a written exception that shall include:

i. A description of why the exception is appropriate, e.g., what business need or circumstance supports the exception;

ii. An assessment of the potential risk posed by the exception; and

iii. A description of the schedule that will be used to evaluate and plan for the application of the security update or patch or addition of any Compensating Controls.

g. In connection with the scheduling and installation of any critical patch and/or update, Blackbaud shall verify that the patch and/or update was applied and installed successfully throughout the Blackbaud Network. For each security update or security patch rated as critical, Blackbaud shall maintain records identifying: (1) each critical patch or update that has been applied; (2) the date(s) each patch or update was applied; (3) the assets to which each patch or update was applied; and (4) whether each patch or update was applied and installed successfully (the "Critical Patch Management Records"). Modifications to the Critical Patch Management Records shall be reviewed on a weekly basis by the Patch Management Group.

h. On a monthly basis, Blackbaud shall perform an internal assessment of its management and implementation of security updates and patches for the Blackbaud Network. This assessment shall identify (i) all known vulnerabilities to the Blackbaud Network and (ii) the updates or patches applied to address each vulnerability. The assessment will be formally identified, documented, and reviewed by the Patch Management Group.

O. Implementation Benchmarks

70. Blackbaud shall maintain a cybersecurity capability roadmap, conduct appropriate planning designed to assist Blackbaud in achieving the cybersecurity capabilities specified on the roadmap, and document progress and completion of projects establishing those cybersecurity capabilities.

VIII. Assessment and Reporting Requirements

71. Blackbaud shall engage an independent third party ("Third-Party Assessor") to conduct assessments of its general data security practices, which includes a risk assessment that complies with HIPAA, as well as its compliance with the terms of this Judgment ("Third-Party Assessments"), as follows:

a. The Third-Party Assessor shall be a Certified Information Systems Security Professional or a Certified Information Systems Auditor, or a similarly qualified person or organization and have at least three (3) years of experience evaluating the effectiveness of computer system security or information system security.

b. The reporting period for the Third-Party Assessments must cover: (1) the first sixty (60) days after the Effective Date for the initial Third-Party Assessment; and (2) every other year thereafter the first Third-Party Assessment for seven (7) years, for a total of four (4) Third-Party Assessments completed in the first, third, fifth, and seventh years after the first Third-Party Assessment. With written pre-approval from Plaintiff, Blackbaud may use the first Third-Party Assessment required by Blackbaud's settlement with the Attorney General of Indiana (effective date of November 6, 2023) to satisfy the first Third-Party Assessment required by this Judgment.

c. The Third-Party Assessments shall:

i. Follow a NIST Cybersecurity Framework or another established industry standard cybersecurity framework;

ii. Identify the specific administrative, technical, and physical safeguards maintained by Blackbaud's Information Security Program;

iii. Document the extent to which the identified administrative, technical and physical safeguards are appropriate considering Blackbaud's size and complexity, the nature and scope of Blackbaud's activities, and the sensitivity of the PI and PHI maintained on the Blackbaud Network; and

iv. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Blackbaud meet the requirements of the Information Security Program and HIPAA.

d. Following each such assessment, the Third-Party Assessor shall prepare a report including its findings and recommendations to cover the requirements under subparagraphs 71.c.i-71.c.iv ("Security Report"), and provide a copy of the Security Report to Blackbaud. A copy of the Security Report shall be provided to the Plaintiff within thirty (30) days of the

completion of the Security Report. With written pre-approval from Plaintiff, Blackbaud may use the first Security Report required by Blackbaud's settlement with the Attorney General of Indiana (effective date of November 6, 2023) to satisfy the first Security Report required by this Judgment.

e. Within ninety (90) days of its receipt of each Security Report, Blackbaud shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the Security Report. Within one hundred eighty (180) days of Blackbaud's receipt of each Security Report, Blackbaud shall forward to the Plaintiff a description of any action they take and, if no action is taken, a detailed description of why no action is necessary, in response to each Security Report.

f. Any Security Report provided pursuant to this Paragraph and all information contained therein, to the extent permitted by the laws of California shall be treated by the Plaintiff as confidential; shall not be shared or disclosed except as permitted by subpart (d) of this Paragraph; and shall be treated by the Plaintiff as exempt from disclosure under the relevant public records laws of the California. In the event that the Plaintiff receives any request from the public for any Security Report provided pursuant to this Paragraph or other confidential documents provided to the Plaintiff under this Judgment, and believes that such information is subject to disclosure under the relevant public records laws, the Plaintiff agrees to provide Blackbaud with at least ten (10) days advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that Blackbaud may take appropriate action to defend against the disclosure of such information. The notice under this Paragraph shall be provided consistent with the notice requirements contained in Paragraph 89. Nothing contained in this subparagraph shall alter or limit the obligations of the Plaintiff that may be imposed by the relevant public records laws of the California, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to the Plaintiff except with respect to the obligation to notify Blackbaud of any potential disclosure.

72. In the event that any audit or other third-party report pertaining to cybersecurity is materially amended or withdrawn, Blackbaud shall immediately notify any Blackbaud Customer or governmental agency with which it has shared the report.

IX. DOCUMENT RETENTION

73. Unless otherwise provided herein, Blackbaud shall retain and maintain any documentation required by Paragraphs 5.h and 14-72 for a period of no less than seven (7) years. In no way does this or any other provision in this Judgment waive any applicable privilege or protection over any Blackbaud document or communication.

MONETARY PROVISION

74. Blackbaud shall pay six million seven hundred and fifty thousand dollars ($6,750,000). Payment shall be made by wire transfer to the California Attorney General's Office pursuant to instructions provided by the Plaintiff. These funds shall be used and allocated in accordance with subdivisions (c) and (d) of Section 17206 of the Business and Professions Code.

RELEASE

75. This Judgment shall have a res judicata effect and shall constitute a full, final, and binding settlement and release, to the fullest extent permitted by law, of each cause of action set forth in the accompanying Complaint that Plaintiff has or could have brought against Blackbaud arising out of 2020 Data Breach. Nothing contained in this paragraph shall be construed to limit the ability of the Plaintiff to enforce the obligations that Blackbaud has under this Judgment. Further, nothing in this Judgment shall be construed to have any affect or impact on any potential or actual claims brought by any consumer or entity against Blackbaud.

NO ADMISSION OF LIABILITY

76. Blackbaud denies wrongdoing or liability of any kind but agreed to resolve the allegations contained in the People's Complaint by entering into this Judgment. Nothing contained in this Judgment is intended to be, and shall not in any event be construed or deemed to be, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Blackbaud or any fact or violation of law, rule, or regulation. This Judgment is made without

trial or adjudication of any alleged issue of fact or law and without any finding of liability or wrongdoing of any kind. Blackbaud enters into this Judgment for settlement purposes only.

ENFORCEMENT

77. This Judgment is entered pursuant to Business and Professions Code section 17200 et seq. Jurisdiction is retained for the purpose of enabling any party to this Judgment with or without the prior consent of the other party to apply to the Court at any time for enforcement of compliance with this Judgment, to punish violations thereof, or to modify or clarify this Judgment.

78. Violation of any of the injunctions contained in this Judgment, as determined by the Court, shall constitute a violation of an injunction for which remedies may be sought by the Attorney General pursuant to Business and Professions Code section 17207 and/or such other remedies as may be provided by law.

79. Blackbaud shall cooperate in good faith with the California Attorney General's Office in any investigation by that office concerning Blackbaud's compliance with this Judgment.

80. If the Attorney General determines that Blackbaud has failed to comply with any of this Judgment, and if in the Attorney General's sole discretion the failure to comply with this Judgment does not threaten the health or safety of the residents of the State of California and/or does not create an emergency requiring immediate action, the Attorney General will notify Blackbaud in writing of such failure to comply and Blackbaud shall have thirty (30) days from receipt of such written notice to provide a good faith written response to the Attorney General, including either a statement that Blackbaud believes it is in full compliance or otherwise a statement explaining how the violation occurred, how it has been addressed or when it will be addressed, and what Blackbaud will do to make sure the violation does not happen again. The Attorney General may agree to provide Blackbaud more than thirty (30) days to respond.

81. In the event the People commence an action to enforce this Judgment, Blackbaud agree that service of any complaint or summons related to enforcement of this Judgment can be served by providing copies of the summons and complaint to Blackbaud's counsel as identified in paragraph 89 below.

82. Nothing in this Judgment shall be construed to limit the authority or ability of the Attorney General to protect the interests of the State of California or the people of the State of California. This Judgment shall not bar the Attorney General or any other governmental entity from enforcing laws, regulations, or rules against Blackbaud for conduct subsequent to or otherwise not covered by this Judgment. Further, nothing in this Judgment shall be construed to limit the ability of the Attorney General to enforce the obligations that Blackbaud has under this Judgment.

83. Nothing in this Judgment shall be construed as relieving Blackbaud of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Judgment be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

GENERAL PROVISIONS

84. Under no circumstances shall this Judgment or the name of the Office of the Attorney General or any of its employees or representatives be used by Blackbaud in connection with any selling, advertising, or promotion of products or services, or as an endorsement or approval of Blackbaud's acts, practices or conduct of business.

85. No court costs, if any, shall be taxed upon the Attorney General. To the extent there are any court costs associated with the filing of this Judgment, Blackbaud shall pay all such court costs.

86. Blackbaud agrees that this Judgment does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and Blackbaud further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

87. This Judgment shall not be construed to waive any claims of sovereign immunity of the State of California may have in any action or proceeding.

88. If any portion of this Judgment is held invalid by operation of law, the remaining terms of this Judgment shall not be affected and shall remain in full force and effect.

89. All notices under this Judgment shall be provided to the following via email and overnight mail:

a. For the People: Darcie Tilly, Deputy Attorney General, Office of the Attorney General, 600 W. Broadway, Suite 1800, San Diego, CA 92101, Darcie.Tilly@doj.ca.gov.

b. For Blackbaud: Sharon Klein, Blank Rome, LLP, 4 Park Plaza, Suite 450, Irvine, CA 92614.

90. This Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Judgment.

91. The clerk is ordered to enter this Judgment forthwith.

IT IS SO ORDERED, this __ day of _____, 2024.

_____

JUDGE OF THE SUPERIOR COURT