

1 ROB BONTA  
Attorney General of California  
2 KATHLEEN BOERGERS  
Acting Senior Assistant Attorney General  
3 KARLI EISENBERG  
Supervising Deputy Attorney General  
4 DARCIE TILLY (SBN 239715)  
Deputy Attorney General  
5 600 West Broadway, Suite 1800  
San Diego, CA 92101  
6 P.O. Box 85266  
San Diego, CA 92186-5266  
7 Telephone: (619) 738-9559  
E-mail: Darcie.Tilly@doj.ca.gov  
8

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

15 *Attorneys for Plaintiff, the People of the State of*  
16 *California*

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

17 SUPERIOR COURT OF THE STATE OF CALIFORNIA

18 COUNTY OF SAN DIEGO

19  
20 PEOPLE OF THE STATE OF CALIFORNIA,  
21 Plaintiff,  
22 v.  
23 BLACKBAUD, INC., a corporation,  
24 Defendant.  
25

Case No.

[PROPOSED] FINAL JUDGMENT AND  
PERMANENT INJUNCTION

26  
27  
28

**TABLE OF CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

	<b>Page</b>
PARTIES AND JURISDICTION.....	1
DEFINITIONS.....	1
INJUNCTION.....	6
I.    Compliance with the Law .....	6
II.   Security Incident Response and Security Incident Response Plan .....	7
III.  Breach Response and Notification.....	7
IV.  Information Security Program.....	9
V.   Training Requirements.....	13
VI.  Personal and Protected Health Information Safeguards and Controls.....	14
VII. Specific Technical Safeguards and Controls.....	15
A.   Network Segmentation.....	15
B.   Risk Assessment .....	16
C.   Penetration and Security Testing .....	16
D.   Access Control and Account Management.....	17
E.   File Integrity Monitoring .....	19
F.   Unauthorized or Malicious Applications .....	19
G.   Logging and Monitoring .....	19
H.   Change Control .....	20
I.   Asset Inventory .....	21
J.   Digital Certificates .....	21
K.   Endpoint Detection and Response (“EDR”).....	22
L.   Intrusion Detection and Prevention Tools.....	22
M.   Threat Management .....	22
N.   Updates and Patch Management .....	22
O.   Implementation Benchmarks .....	26
VIII. Assessment and Reporting Requirements.....	26
IX.  Document Retention.....	29
MONETARY PROVISION.....	29
RELEASE .....	29
NO ADMISSION OF LIABILITY .....	29
ENFORCEMENT .....	30
GENERAL PROVISIONS .....	31

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

9 **IT IS HEREBY ORDERED, ADJUDGED AND DECREED THAT:**

10 **PARTIES AND JURISDICTION**

- 11 1. The People of the State of California is the Plaintiff in this case.
- 12 2. Blackbaud, Inc. is the Defendant in this case. Blackbaud is a Delaware corporation  
13 with its principal office located at 65 Fairchild Street, Charleston, South Carolina 29492.
- 14 3. This Court has jurisdiction over the allegations and subject matter of the People’s  
15 Complaint filed in this action, and the parties to this action; venue is proper in this County; and  
16 this Court has jurisdiction to enter this Judgment and to enforce its provisions.
- 17 4. Jurisdiction is proper because Blackbaud has transacted business within the State  
18 of California, and San Diego County, and/or has engaged in conduct impacting the State of  
19 California or its residents at all times relevant to the claims at issue.

20 **DEFINITIONS**

- 21 5. In addition to terms defined elsewhere in the Judgment, for the purposes of this  
22 Judgment:
- 23 a. “2020 Data Breach” shall mean the Security Incident, first publicly  
24 announced by Blackbaud on July 16, 2020, in which a person or persons gained unauthorized  
25 access to the Blackbaud Network.
- 26 b. Blackbaud shall include Blackbaud and its directors, officers, employees,  
27 representatives, agents, affiliates, parents, subsidiaries, predecessors, assigns, and successors.
- 28

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

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

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

13 f. “Business Associate” shall be defined in accordance with 45 C.F.R. §  
14 160.103.

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

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

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

27  
28

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

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

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

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

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

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

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

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

14 j. “Consumer Protection Laws” shall mean Business and Professions Code  
15 section 17200 et seq. and Business and Professions Code section 17500 et seq.

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

17 l. “Data Breach Notification Law” shall mean Civil Code § 1798.82.

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

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

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

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

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

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

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

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

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

19 r. "Personal Information Protection Law" shall mean Civil Code section  
20 1798.81.5.

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

23 t. "Security Incident" shall mean any compromise, or imminent threat of a  
24 compromise to the confidentiality, integrity, or availability of PI or PHI stored within, accessed,  
25 or transmitted through the Blackbaud Network, by unauthorized access or inadvertent disclosure,  
26 including but not limited to an incident for which notification may be required under the Data  
27 Breach Notification Law or HIPAA. For purposes of this definition, "availability" shall not  
28

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

### 3 **INJUNCTION**

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

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

#### 9 **I. COMPLIANCE WITH THE LAW**

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

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

14 10. Blackbaud shall comply with HIPAA, as applicable, including the Privacy Rule  
15 (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  
16 160 and 45 C.F.R. Part 164, Subparts A and C), and shall implement all Administrative,  
17 Technical, and Physical Safeguards required by HIPAA. “Administrative Safeguards”,  
18 “Technical Safeguards” and “Physical Safeguards” shall be defined in accordance with 45 C.F.R.  
19 §§ 164.304, 164.308, 164.310, 164.312.

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

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



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

3     **II.   SECURITY INCIDENT RESPONSE AND SECURITY INCIDENT RESPONSE PLAN**

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

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

- 7           a.     Preparation;
- 8           b.     Detection and Analysis;
- 9           c.     Containment;
- 10          d.     Eradication;
- 11          e.     Recovery; and
- 12          f.     Post-Incident Analysis and Remediation.

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

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

23     **III.   BREACH RESPONSE AND NOTIFICATION**

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

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

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

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

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

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

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

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

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

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

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

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

21 **IV.   INFORMATION SECURITY PROGRAM**

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

- 1 a. The size and complexity of Blackbaud's operations;
- 2 b. The nature and scope of Blackbaud's activities; and
- 3 c. The sensitivity of the PI and PHI on the Blackbaud Network.

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

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

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

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

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

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

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

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

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

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

26 31. Blackbaud shall employ an executive or officer who shall be responsible for  
27 implementing, maintaining, and monitoring the Information Security Program (hereinafter  
28

1 referred to as the “Chief Information Security Officer”). The Chief Information Security Officer  
2 shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 25 **V. TRAINING REQUIREMENTS**

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

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

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

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

17 **VI. PERSONAL AND PROTECTED HEALTH INFORMATION SAFEGUARDS AND CONTROLS**

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

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



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

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

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

## 18 **VII. SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS**

### 19 **A. Network Segmentation**

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

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

26 45. Blackbaud shall logically separate its development, production and non-production  
27 environments in the Blackbaud Network.  
28

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

5           **B.     Risk Assessment**

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

18           **C.     Penetration and Security Testing**

19           48.     Within sixty (60) days of the Effective Date, Blackbaud shall implement and  
20 maintain a risk-based security-testing program reasonably designed to identify, assess, and  
21 remediate security vulnerabilities within the Blackbaud Network. This program shall include: (i)  
22 testing for security vulnerabilities for Blackbaud developed applications before deployment to  
23 any public-facing webserver using static and dynamic application testing for production releases;  
24 (ii) at least one annual penetration test of all Blackbaud products; (iii) vulnerability scans of all  
25 systems in the Blackbaud Network occurring at least weekly; and (iv) vulnerability scans of the  
26 production environment of the Blackbaud Network within twenty-four (24) hours after any  
27 material modifications. All results shall be documented and maintained for two (2) years.  
28

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

12           **D.     Access Control and Account Management**

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

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

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

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

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

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

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

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

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

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

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

5 **E. File Integrity Monitoring**

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

11 **F. Unauthorized or Malicious Applications**

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

14 **G. Logging and Monitoring**

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

20 61. All Security Incidents shall promptly be reported to the Chief Information Security  
21 Officer and the Office of the Chief Privacy Officer consistent with the timeframes specified in the  
22 Blackbaud Incident Response Plan which, to the extent applicable, shall be aligned to NIST 800-  
23 61r2 and include processes for communicating Security Incidents to the appropriate leaders,  
24 executives, and committees to appropriately manage the risk. Any critical vulnerability that is  
25 associated with a Security Incident shall be remediated within twenty-four (24) hours of the  
26 identification of such vulnerability. If that vulnerability cannot be remediated as indicated above,  
27 then Blackbaud shall within twenty-four (24) hours of the identification of such vulnerability: (a)  
28 implement Compensating Controls; or (b) take the application or functionality of the application

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

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

#### 7 **H. Change Control**

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

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

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

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

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

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

### 8 **I. Asset Inventory**

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

### 19 **J. Digital Certificates**

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

1           **K. Endpoint Detection and Response (“EDR”)**

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

9           **L. Intrusion Detection and Prevention Tools**

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

14          **M. Threat Management**

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

19          **N. Updates and Patch Management**

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

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



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

- 5 i. A description of why the exception is appropriate, e.g., what  
6 business need or circumstance supports the exception;
- 7 ii. An assessment of the potential risk posed by the exception; and
- 8 iii. A description of the schedule that will be used to evaluate and plan  
9 for the replacement of the software or addition of any Compensating Controls.

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

- 12 i. Maintain a patch management solution(s) to manage software  
13 patches that includes the use of standardized patch management distribution tool(s), including  
14 automation-assisted processes, whenever appropriate; and
- 15 ii. Maintain a tool that includes an automated Common Vulnerabilities  
16 and Exposures (“CVE”) feed. The CVE tool required by this subparagraph shall provide  
17 Blackbaud regular updates, including daily updates to the extent available, regarding known  
18 CVEs for vendor-purchased software applications in use within the Blackbaud Network.

19 Blackbaud may satisfy its obligations under this subparagraph by using an industry-standard  
20 vulnerability scanning tool. The CVE tool required by this subparagraph shall also:

- 21 1. Identify, confirm, and enhance discovery of the parts of the  
22 Blackbaud Network that may be subject to CVE events and/or incidents;
- 23 2. Scan the Blackbaud Network for CVEs; and
- 24 3. Scan the Blackbaud Network to determine whether  
25 scheduled security updates and patches have been successfully installed, including whether any  
26 security updates or patches rated as critical have been installed consistent with the requirement of  
27 this Judgment.

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

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

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

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

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

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

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

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

- 8 i. A description of why the action is appropriate, e.g., what business  
9 need or circumstance exists that supports the rating;
- 10 ii. A description of the alternatives that were considered, and why they  
11 were not appropriate;
- 12 iii. An assessment of the potential risks posed by the action;
- 13 iv. The anticipated length of time for the action, if the action is  
14 temporary; and
- 15 v. To the extent applicable, a plan for managing or mitigating those  
16 risks identified in subparagraph (69.e.iii) (e.g., Compensating Controls, alternative approaches,  
17 methods). The written explanation required by this subparagraph shall be prepared within forty-  
18 eight (48) hours of its determination to apply an exception.

19 f. Blackbaud shall, within a time period appropriate to the risk to the  
20 Blackbaud Network, but not later than forty-eight (48) hours of rating any security update or  
21 patch as critical or critical zero-day, either: (1) apply such update or patch to the Blackbaud  
22 Network; (2) apply Compensating Controls; or (3) if Blackbaud is unable to timely update or  
23 patch the Blackbaud Network, or apply Compensating Controls, Blackbaud will take the  
24 identified application or affected functionality of the identified application offline until the update  
25 or patch or Compensating Controls has been successfully applied. If Blackbaud chooses not to  
26 apply such update or patch to the Blackbaud Network and instead to implement Compensating  
27 Controls, it shall prepare and maintain a written exception that shall include:  
28

- 1                   i.           A description of why the exception is appropriate, e.g., what  
2 business need or circumstance supports the exception;
- 3                   ii.           An assessment of the potential risk posed by the exception; and
- 4                   iii.           A description of the schedule that will be used to evaluate and plan  
5 for the application of the security update or patch or addition of any Compensating Controls.
- 6                   g.           In connection with the scheduling and installation of any critical patch  
7 and/or update, Blackbaud shall verify that the patch and/or update was applied and installed  
8 successfully throughout the Blackbaud Network. For each security update or security patch rated  
9 as critical, Blackbaud shall maintain records identifying: (1) each critical patch or update that has  
10 been applied; (2) the date(s) each patch or update was applied; (3) the assets to which each patch  
11 or update was applied; and (4) whether each patch or update was applied and installed  
12 successfully (the “Critical Patch Management Records”). Modifications to the Critical Patch  
13 Management Records shall be reviewed on a weekly basis by the Patch Management Group.
- 14                   h.           On a monthly basis, Blackbaud shall perform an internal assessment of its  
15 management and implementation of security updates and patches for the Blackbaud Network.  
16 This assessment shall identify (i) all known vulnerabilities to the Blackbaud Network and (ii) the  
17 updates or patches applied to address each vulnerability. The assessment will be formally  
18 identified, documented, and reviewed by the Patch Management Group.

19                   **O.   Implementation Benchmarks**

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

24                   **VIII. ASSESSMENT AND REPORTING REQUIREMENTS**

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

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

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

13           c.       The Third-Party Assessments shall:

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

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

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

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

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

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

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

11 f. Any Security Report provided pursuant to this Paragraph and all  
12 information contained therein, to the extent permitted by the laws of California shall be treated by  
13 the Plaintiff as confidential; shall not be shared or disclosed except as permitted by subpart (d) of  
14 this Paragraph; and shall be treated by the Plaintiff as exempt from disclosure under the relevant  
15 public records laws of the California. In the event that the Plaintiff receives any request from the  
16 public for any Security Report provided pursuant to this Paragraph or other confidential  
17 documents provided to the Plaintiff under this Judgment, and believes that such information is  
18 subject to disclosure under the relevant public records laws, the Plaintiff agrees to provide  
19 Blackbaud with at least ten (10) days advance notice before producing the information, to the  
20 extent permitted by state law (and with any required lesser advance notice), so that Blackbaud  
21 may take appropriate action to defend against the disclosure of such information. The notice  
22 under this Paragraph shall be provided consistent with the notice requirements contained in  
23 Paragraph 89. Nothing contained in this subparagraph shall alter or limit the obligations of the  
24 Plaintiff that may be imposed by the relevant public records laws of the California, or by order of  
25 any court, regarding the maintenance or disclosure of documents and information supplied to the  
26 Plaintiff except with respect to the obligation to notify Blackbaud of any potential disclosure.  
27  
28

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

4 **IX. DOCUMENT RETENTION**

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

9 **MONETARY PROVISION**

10           74. Blackbaud shall pay six million seven hundred and fifty thousand dollars  
11 (\$6,750,000). Payment shall be made by wire transfer to the California Attorney General's Office  
12 pursuant to instructions provided by the Plaintiff. These funds shall be used and allocated in  
13 accordance with subdivisions (c) and (d) of Section 17206 of the Business and Professions Code.

14 **RELEASE**

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

22 **NO ADMISSION OF LIABILITY**

23           76. Blackbaud denies wrongdoing or liability of any kind but agreed to resolve the  
24 allegations contained in the People's Complaint by entering into this Judgment. Nothing  
25 contained in this Judgment is intended to be, and shall not in any event be construed or deemed to  
26 be, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part  
27 of Blackbaud or any fact or violation of law, rule, or regulation. This Judgment is made without  
28

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

### 3 **ENFORCEMENT**

4 77. This Judgment is entered pursuant to Business and Professions Code section  
5 17200 et seq. Jurisdiction is retained for the purpose of enabling any party to this Judgment with  
6 or without the prior consent of the other party to apply to the Court at any time for enforcement of  
7 compliance with this Judgment, to punish violations thereof, or to modify or clarify this  
8 Judgment.

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

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

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

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





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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