UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of **BLACKBAUD, INC., a corporation**.	**DOCKET NO. C-4804**

COMPLAINT

The Federal Trade Commission, having reason to believe that Blackbaud, Inc., a corporation, ("Blackbaud"), has violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Blackbaud, Inc. is a Delaware corporation with its principal place of business at 65 Fairchild Street, Charleston, South Carolina 29492.

2. The acts and practices of Blackbaud alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, and constitute unfair and/or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

Summary of the Case

3. Blackbaud failed to use appropriate information security practices to protect consumers' personal information. These failures allowed an attacker to access Blackbaud's customer databases and steal personal information relating to millions U.S. consumers, as described in greater detail below.

Blackbaud's Business Practices

4. Blackbaud provides a variety of data services and financial, fundraising, and administrative software services to its customers, more than 45,000 companies, nonprofits, foundations, educational institutions, healthcare organizations, and individual consumers throughout the U.S. and abroad. It maintains a wide variety of consumers' personal information on behalf of its customers, as described below in Paragraph 8.

5. Blackbaud generates most of its U.S. revenues primarily from software solutions in cloud and hosted environments; payment and transaction services; software maintenance and support services; and professional services, including implementation, consulting, training, and analytic services. It earned annual revenues of approximately $1.1 billion in 2022.

Data Breach

6. On February 7, 2020, an attacker gained access to Blackbaud's self-hosted legacy product databases. The attacker remained undetected for over three months, until May 20, 2020, when a member of Blackbaud's engineering team identified a suspicious login on a backup server. By the time Blackbaud discovered the breach, the attacker had stolen data from tens of thousands of Blackbaud's customers, which comprised of the personal information of millions of consumers.

7. The attacker purportedly used a Blackbaud customer's login and password to access the customer's Blackbaud-hosted database. Once logged in, the attacker was able to freely move across multiple Blackbaud-hosted environments by leveraging existing vulnerabilities and local administrator accounts, subsequently creating new administrator accounts and ultimately exfiltrating massive amounts of consumer data belonging to Blackbaud's customers.

8. Blackbaud's investigation found that the attacker had exfiltrated files in which millions of consumers' personal information was not encrypted, including consumers' full names, age, date of birth, social security numbers, home addresses, phone numbers, email addresses, financial information (including bank account information, estimated wealth, and identified assets), medical information (including patient and medical record identifiers, treating physician names, health insurance information, medical visit dates, and reasons for seeking medical treatment), gender, religious beliefs, marital status, spouse names, spouses' donation history, employment information (including salary) educational information, and account credentials.

9. Blackbaud's deficient encryption practices magnified the severity of the data breach. For example, Blackbaud allowed customers to store social security numbers and bank account information in unencrypted fields not specifically designated for those purposes. It also allowed customers to upload attachments containing consumers' personal information, which Blackbaud did not encrypt. Finally, Blackbaud did not encrypt its database backup files which contained complete customer records from the products' databases, even for former customers.

10. Blackbaud's failure to implement appropriate data retention policies further exacerbated the severity of the breach. Blackbaud did not enforce its own data retention policies, resulting in the company keeping customer's consumer data for years longer than was necessary. Incredibly, in some instances, Blackbaud retained data belonging to former

customers, customers who had switched to products not affected by the breach, and even potential customers for years longer than was necessary.

11. Once detected, the attacker threatened to expose the stolen consumer data unless Blackbaud paid a ransom. Blackbaud eventually agreed to pay 24 Bitcoin (valued at $235,000 at the time) in exchange for the attacker's promise to delete the stolen data. Blackbaud has not been able to conclusively verify that the attacker deleted the stolen data.

Blackbaud's Deceptive Breach Notification Statements

12. Blackbaud failed to notify its customers of the breach for two months after detection. It issued its first notice to its customers on July 16, 2020.

13. However, in its July 2020 breach notification, Blackbaud misrepresented the scope and severity of the breach after conducting an exceedingly inadequate investigation. Blackbaud stated in its communications to customers:

> The cybercriminal did not access credit card information, bank account information, or social security numbers. . .
>
> **No action is required on your end because no personal information about your constituents was accessed**. (emphasis in original)
>
> (Exhibit A, Sample Blackbaud Customer Breach Notification (July 16, 2020))

14. Although Blackbaud knew, as early as July 31, 2020, as part of its continuing post-breach investigation, that the attacker had exfiltrated consumers' bank account numbers and social security numbers, Blackbaud did not disclose the extent of the breach to its customers until October 2020.

15. Blackbaud's deceptive statements, combined with the months' long delay in providing accurate notice about the breach, led many customers to believe that notification to their consumers was unnecessary. Due to this delay in notice, consumers suffered additional harm because they had no way to know that they needed to take any mitigating steps to protect themselves from identity theft.

16. Since the breach, Blackbaud has received multiple complaints from consumers involving attempted identity theft and fraud using the personal information exposed in the breach (e.g., credit card, tax, and unemployment fraud). Blackbaud has since offered credit monitoring services to a limited subset of affected customers.

Blackbaud's Deceptive Information Security Statements

17. Blackbaud has made explicit representations about its information security practices that led customers to believe that it used reasonable and appropriate information security practices to protect consumers' personal information.

18. Blackbaud's Privacy Policy on its website, dated December 17, 2019, included the following statement:

> **Security of your Personal Information**. We restrict access to personal information collected about you at our website to our employees, our affiliates' employees, those who are otherwise specified in this Policy or others who need to know that information to provide the Services to you or in the course of conducting our business operations or activities. While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons. We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company's business ethics standards and confidentiality policies. Inside Blackbaud, data is stored in password-controlled servers with limited access.
>
> (**Exhibit B**, Blackbaud.com, Privacy Policy North America (December 17, 2019))

Blackbaud's Information Security Practices

19. Blackbaud failed to provide reasonable or appropriate security for the personal information that they collected and maintained about consumers. Among other things, Blackbaud failed to:

    a. Implement appropriate password controls. As a result of this failure, employees often used default, weak, or identical passwords;

    b. Apply adequate multifactor authentication for both employees and customers to protect sensitive consumer information. For example, Blackbaud failed to comply with industry standards and internal policies requiring multifactor authentication for remote access to sensitive environments;

    c. Prevent data theft by monitoring for unauthorized attempts to transfer or exfiltrate consumers' personal information outside the company's networks; continuously log and monitor its systems and assets to identify

data security events; and perform regular assessments as to the effectiveness of protection measures;

d. Implement and enforce appropriate data retention schedules and deletion practices for the vast amounts of consumers' personal information stored on its network;

e. Patch outdated software and systems in a timely manner, leaving Respondents' networks susceptible to attacks;

f. Test, audit, assess, or review its products' or applications' security features; and conduct regular risk assessments, vulnerability scans, and penetration testing of its networks and databases;

g. Implement appropriate firewall controls. This failure resulted in an attacker making unauthorized connections from outside of Respondents' networks; and

h. Implement appropriate network segmentation to prevent attackers from moving freely across Blackbaud's networks and databases.

The Impact of Blackbaud's Failures on Consumers

20. Respondent's failures to provide reasonable security for the sensitive, personal consumer information they collected, transmitted, and stored has caused or is likely to cause substantial injury to consumers.

21. Additionally, Blackbaud's failure to accurately communicate the scope and severity of the breach in its initial notification to its customers caused or is likely to cause substantial injury to consumers because they were not able to mitigate the effects of the breach in a timely manner.

22. Consumers have also suffered, and will continue to suffer, additional injuries due to the significant amount of highly detailed and individualized personal information exposed.

23. Blackbaud could have prevented or mitigated these failures described in Paragraph 19 through well known, readily available, relatively low-cost measures. For example, Blackbaud could have required regular review of access permissions, enabled multi-factor authentication for all employees and customers, and implemented reasonable data retention practices. Any of these measures would likely have prevented the May 2020 breach or, at minimum, lessened its impact.

24. These harms were not reasonably avoidable by consumers, as consumers had no way to know about Respondents' information security failures described in Paragraph 19 above.

Violation of the FTC Act

25. The acts and practices of Respondent, as alleged in this Complaint, constitute unfair and/or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

Count I – Blackbaud's Unfair Information Security Practices

26. Through the means described in Paragraphs 6 to 11 and 19-24, Blackbaud failed to take reasonable steps to prevent unauthorized access to sensitive consumer data maintained by its customers on its network.

27. Blackbaud's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

28. Therefore, Blackbaud's practices as described in Paragraph 19 above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

Count II – Blackbaud's Unfair Data Retention Practices

29. Through the means described in Paragraph 10, Blackbaud failed to implement and enforce reasonable data retention practices for sensitive consumer data maintained by its customers on its network.

30. Blackbaud's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

31. Therefore, Blackbaud's practices as described in Paragraph 19(d) above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

Count III—Blackbaud's Unfair Inaccurate Breach Notification

32. Through the means described in Paragraphs 12 to 16 and 21, Blackbaud failed to accurately communicate the scope and severity of the breach in its initial notification to customers.

33. Blackbaud's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumer or competition.

34. Therefore, Blackbaud's practices described in Paragraphs 12 and 13 above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

Count IV – Blackbaud's Deceptive Security Statements

35. Through the means described in Paragraphs 17 to 18, Blackbaud has represented, directly or indirectly, expressly or by implication, that they used appropriate safeguards to protect consumers' personal information.

36. In truth and in fact, as set forth in Paragraph 19, Blackbaud did not maintain appropriate safeguards to protect consumers' personal information. Therefore, the representation set forth in Paragraph 18 is false or misleading.

Count V – Blackbaud's Deceptive Initial Breach Notification

37. Through the means described in Paragraph 12 to 13, Blackbaud has represented, directly or indirectly, expressly or by implication, that consumers' personal information had not been subject to the breach in its first notification.

38. In truth and in fact, as set forth in Paragraphs 14 to 16, consumers' personal information had been exfiltrated by the attacker in the breach. Therefore, the representation set forth in Paragraph 13 is false or misleading.

THEREFORE, the Federal Trade Commission this 17th day of May, 2024 has issued this complaint against Respondent.

By the Commission, Commissioner Ferguson not participating and Commissioner Holyoak recused.

April J. Tabor
Secretary

SEAL:

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of **BLACKBAUD, INC., a corporation.**	**DECISION AND ORDER** **DOCKET NO. C-4804**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondents that it neither admits nor denies any of the allegations in the draft Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of thirty (30) days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order. The parties agree that this Order resolves all allegations in the Complaint:

Findings

1. Respondent Blackbaud, Inc. ("Blackbaud") a Delaware corporation with its principal place of business at 65 Fairchild Street, Charleston, South Carolina 29492.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

Definitions

1. "**Covered Incident**" means any incident that results in Respondent notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

2. "**Covered Information**" means information from or about an individual consumer stored by Respondent's customers within Respondent's product databases including: (a) a first and last name: (b) a home or physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) a driver's license or other government-issued identification number; (f) date of birth; or (g) bank account, credit card, or debit card information.

3. "**Delayed Update Customers**" are Respondent's customers to whom Respondent makes updates available but who do not automatically implement such updates due to the complexity of Respondent's customers implementing such updates into Respondent's customers' environments and business practices.

4. "**Delete**" "**Deleted**" or "**Deletion**" means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

5. **"Respondent"** means Blackbaud, Inc., a Delaware corporation, and its successors and assigns.

Provisions

I. Prohibition against Misrepresentations about Privacy and Security

IT IS ORDERED that Respondent, Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them who receive

actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

A. The extent to which Respondent maintains, uses, Deletes, or discloses any Covered Information;

B. The extent to which Respondent protects the privacy, security, availability, confidentiality, or integrity of any Covered Information; or

C. The extent of any Covered Incident or unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of Covered Information.

II. Mandated Data Deletion

IT IS FURTHER ORDERED that Respondent must:

A. Within 90 days after the Order Effective Date, Delete or destroy Respondent customer backup files containing Covered Information that is not being retained in connection with providing products or services to Respondent's customers unless otherwise requested by Respondent's customers, and provide a written statement to the Commission, pursuant to the Provision entitled Compliance Reports and Notices, confirming that all such data has been Deleted or destroyed, specifically enumerating which types of information were Deleted or destroyed; and

B. Refrain from maintaining any Covered Information not necessary for the purpose(s) for which such information is stored and/or maintained by Respondent.

Provided, however, that any Covered Information that any Respondent is otherwise required to Delete or destroy pursuant to this provision may be retained, and may be disclosed, as requested by a government agency or otherwise required by law, regulation, court order, or other legal obligation, including as required by rules applicable to the safeguarding of evidence in pending litigation. In each written statement to the Commission required by this provision, such Respondent shall describe in detail any Covered Information that Respondent retains on any of these bases and the specific government agency, law, regulation, court order, or other legal obligation that prohibits Respondent from deleting or destroying such information. Within thirty (30) days after the obligation to retain the information has ended, Respondent shall provide an additional written statement to the Commission, sworn under penalty of perjury, confirming that Respondent has deleted or destroyed such information.

III. Data Retention Limits

IT IS FURTHER ORDERED that Respondent, in connection with the storage, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 90 days of the Order Effective Date, document, make publicly available on its website(s), and adhere to a retention schedule for Respondent customer backup files containing Covered Information, setting forth: (1) the purpose or purposes for which Covered Information is maintained by Respondent; (2) the specific business needs for Respondent retaining such Covered Information; and (3) a set timeframe for Deletion of Covered Information that precludes indefinite retention of any Covered Information. For clarity, the requirements of this Provision III.A shall additionally apply to the databases containing the Covered Information of former customers and customers who migrate to a different Respondent product; and

B. Within 90 days after the Order Effective Date, provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Respondent customer backup files containing Covered Information made publicly available on its website(s).

IV. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, and any business that Respondent controls directly, or indirectly in connection with the maintenance, use, or disclosure of, or provision of access to, Covered Information, must, within ninety (90) days of the Order Effective Date, establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, confidentiality, and integrity of such Covered Information ("**Information Security Program**"). Delayed Update Customers are exempt from the initial 90-day timing requirement, but Respondent will assist Delayed Update Customers, upon their approval, to update their software in a timely manner. To satisfy this requirement, Respondent must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Provide the written Information Security Program and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in: (1) the

unauthorized storage, maintenance, alteration, use, or disclosure of, or provision of access to, Covered Information; or (2) the misuse, loss, theft, and unauthorized alteration, destruction, or other compromise of Covered Information;

E. Design, implement, maintain, and document safeguards within Respondent's control that control for the internal and external risks Respondent identifies to the security, confidentiality, or integrity of Covered Information identified in response to sub-Provision D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in: (1) the unauthorized storage, maintenance, use, or disclosure of, or provision of access to, Covered Information; or (2) the misuse, loss, theft, and unauthorized alteration, destruction, or other compromise of Covered Information. Such safeguards must also include:

    1. A written information security policy and accompanying written standards or procedures that describe, at a minimum: (a) how Respondent implements each of the safeguards identified in this sub-Provision; and (b) how Respondent assesses and enforces compliance with these safeguards and any other controls it identifies in the policy and accompanying standards and procedures;

    2. Standards, procedures, and policy provisions mandating security education that address internal or external risks Respondent identifies under sub-Provision D of this Provision, and that includes, at a minimum: (a) training for Respondent's employees about Respondent's security policy, standards, and procedures, including the requirements of this Order and the process for submitting complaints and concerns, to be conducted when an employee begins employment or takes on a new role, and on at least an annual basis thereafter; and (b) training in secure software development principles, including secure engineering and defensive programming concepts, for developers, engineers, system administrators, and other employees that design, implement, and operate Respondent's products or services or that are otherwise responsible for the security of Covered Information;

    3. Policy provisions and, to the extent possible, technical measures requiring Respondent's employees or contractors, or third parties to secure any accounts with access to a Respondent's information technology infrastructure by: (a) using strong, unique passwords; and (b) preventing password reuse and password rotation through implementing appropriate tools;

    4. Requiring multi-factor authentication methods for all employees and contractors of Respondent and its affiliates in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all

employees and contractors of Respondent and its affiliates shall not include telephone or SMS-based authentication methods and must be resistant to phishing attacks. Respondent may use widely adopted industry authentication options that provide at least equivalent security as the multi-factor authentication options required by this sub-Provision, if approved in writing by the Commission;

5. Requiring multi-factor authentication methods for all Respondent's customers, except for those customers who use enterprise single sign on solutions within their organizations to access Respondent products and for Delayed Update Customers. However, Respondent shall make available an update for multi-factor authentication methods for Delayed Update Customers;

6. Technical measures, standards, procedures, and policy provisions to: (a) log and monitor access to repositories of Covered Information; (b) limit access to Covered Information by, at a minimum, limiting Respondent employee and service provider access to what is needed to perform that employee's or service provider's job function; (c) grant and audit varying levels of access based on an employee's need to know; and (d) periodically monitor and terminate employee and contractor accounts following inappropriate usage or termination of employment;

7. Technical measures, standards, procedures, and policy provisions to control access to Respondent's customer databases containing Covered Information, including, at a minimum: (a) for Respondent's and its affiliates' employees and contractors, restrictions of inbound connections to those originating from approved IP addresses, such as corporate VPN; (b) requiring connections to be authenticated and encrypted; and (c) periodic audits of account permissions;

8. Technical measures, standards, procedures, and policy provisions relating to Covered Information which: (a) monitor and log transfers or exfiltration of Covered Information from Respondent's network boundaries; (b) monitor and log data security events and other anomalous activity; and (c) verify the effectiveness of monitoring and logging;

9. Technical measures to safeguard against unauthorized access to Covered Information, including: (a) an intrusion prevention or detection system; (b) file integrity monitoring tools; (c) data loss prevention tools; (d) properly configured firewalls; and (e) properly configured physical or logical segmentation of networks, systems and databases;

10. Authentication procedures designed to prevent one customer's credentials from accessing another customer's data or other unauthorized areas in Respondent's networks;

11. Technical measures, procedures, and policy provisions to systematically inventory assets (including databases) storing Covered Information and Delete Respondent customer backup files containing Covered Information that is no longer necessary;

12. Encryption of, at a minimum, fields in Respondent's products designed to store Social Security numbers, passport numbers, tax ID information, driver's license or other government-issued identification numbers; bank account, credit card, or debit card information, dates of birth associated with a consumer, Medical Information associated with a consumer, and user account credentials on Respondent's computer networks, including but not limited to cloud storage;

13. Technical measures, procedures, and policy provisions to address the maintenance of any new type of information related to consumers that was not being maintained as of the issuance data of this Order, including: (a) the purposes or purposes for which the new information is maintained; (b) the specific business needs for maintaining the new information; and (c) encryption of sensitive consumer information; and

14. Enforcing policies and procedures consistent with this Order designed to ensure the timely investigation of data security events and the timely remediation of critical and high-risk security vulnerabilities relating to Covered Information.

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, or integrity of Covered Information, and modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards specified in this Provision at least once every twelve (12) months and promptly (not to exceed 30 days) following a Covered Incident and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability scanning of Respondent's network(s) containing Covered Information once every four months and promptly (not to exceed 30 days) after a Covered Incident, and penetration testing of Respondent's network(s) containing Covered Information at least once every twelve (12) months and promptly (not to exceed 30 days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to

implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Information Security Program in light of any material changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision IV.D of this Order, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

V. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision IV of this Order titled Mandated Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment: and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may satisfy the requirements to obtain Assessments through the use of assessments that are also intended to meet the requirements of other regulatory mandates to which Respondent is subject, provided that such assessments meet the requirements of the Information Security Program set forth in this Order.

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in their sole discretion.

C. The reporting period for the Assessments must cover: (1) at least the first 180 days after the Information Security Program is established for the initial Assessment; and (2) each 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Information Security Program required by Provision IV of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions IV.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and (5) identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondent's management, and state the number of hours that each member of the Assessor's assessment team worked on the Assessment. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision IV of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. The initial Assessment must be completed within one hundred and twenty (120) days after the end of the reporting period for the initial Assessment. Each subsequent biennial Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Blackbaud, FTC File No. 2023181." All subsequent biennial Assessments must be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

VI. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision V of this Order titled Information Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege.

B. Provide or otherwise make available to the Assessor information about Respondent's network(s) and all of Respondent's IT assets that maintain Covered Information so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Information Security Program required by Provision IV of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions IV.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

VII. Annual Certification

IT IS FURTHER ORDERED that Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from Respondent's Chief Information Security Officer responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Blackbaud, FTC File No. 2023181."

VIII. Covered Incident Reports

IT IS FURTHER ORDERED that, within ten (10) days of any notification to a United States federal, state, or local entity of a Covered Incident, Respondent must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of Respondent's customers affected by the Covered Incident;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Respondent to its customers, or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Blackbaud Inc, FTC File No. 2023181."

IX. Order Acknowledgements

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within 10 days after the Order Effective Date, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 20 years after issuance of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, and directors; (2) all employees having managerial responsibilities for cybersecurity, privacy, and the collection, use, or disclosure of Covered Information, and all agents and representatives who participate in cybersecurity, privacy, and the collection, use, or disclosure of Covered Information; and (3) any business entity resulting from any change in structure as set forth in Provision X.

Delivery must occur within 10 days of the Order Effective Date for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

X. Compliance Reporting

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One year after issuance of this Order, Respondent must submit a compliance report, sworn under penalty of perjury. Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For 20 years after issuance of this Order, Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by

overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Blackbaud, Inc."

XI. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after issuance of the Order and retain each such record for 5 years. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services relating to Covered Information, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all consumer complaints regarding security, privacy, or identity theft related to Covered Information whether received directly or indirectly, such as through a third party, and any response;

D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and

E. A copy of each widely disseminated, unique advertisement or other marketing material that references or otherwise relates to Respondent's privacy and data security practices.

XII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions and produce documents for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission is authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview any employee or other person affiliated with

Respondent who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order (the "**Order Effective Date**"). This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Ferguson not participating and Commissioner Holyoak recused.

April J. Tabor
Secretary

SEAL:
ISSUED: May 17, 2024

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

May 17, 2024

Chris Frascella
Suzanne Bernstein
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Re: *In the Matter of Blackbaud, Inc.*, File No. 2023181

Dear Electronic Privacy Information Center:

Thank you for your comment regarding the Federal Trade Commission's ("FTC") proposed consent agreement in the above-titled proceeding against Blackbaud, Inc. ("Blackbaud").

The complaint in this matter alleges that Blackbaud engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges that Blackbaud: (1) failed to employ reasonable information security practices to protect consumers' personal information; (2) failed to implement and enforce reasonable data retention practices; (3) failed to accurately communicate about the breach in its initial notification to customers; (4) misrepresented that it used appropriate safeguards to protect consumers' personal information; and (5) misrepresented the scope of the breach by stating that consumers' personal information had not been impacted by the breach in its initial notification.

Your comment indicates support for the FTC's proposed consent agreement with Blackbaud and praises the FTC for exercising its authority to investigate and take enforcement actions against companies that engage in unfair and deceptive practices. Additionally, your comment provides recommendations to strengthen the proposed order and future data security enforcement actions.

Specifically, your comment supports the proposed order's data minimization and third-party oversight requirements, as well as the novel injunctive relief addressing Blackbaud's initial breach notification to its customers. However, you also raise a concern that the mishandling of personal data by donor management platforms such as Blackbaud may cause a donor "chilling effect," as donors may fear exposure to privacy risks associated with charitable giving. To combat this potential concern, you suggest the FTC hold vendors that provide services to non-profit organizations to the same, or more rigorous, standards as other commercial actors.

The Commission is committed to vigorously enforcing the proposed order and ensuring that all companies that engage in deceptive and unfair practices be held fully accountable, including vendors that provide services to non-profit organizations. Several data security

safeguards in the proposed order help ensure consumers' personal information is protected. For instance, the proposed order requires Blackbaud to regularly train its employees on its information security program and implement technical measures, such as monitoring and logging transfers or exfiltration of personal information within Blackbaud's network. Furthermore, the proposed order requires multi-factor authentication methods for all Blackbaud employees, contractors, and Blackbaud's customers.

As you highlight in your comment, the proposed order also requires Blackbaud to delete or destroy its customer backup files containing personal information that is not being retained in connection with providing products or services to its customers. While you express support for the data deletion mandate, you suggest that the Commission "extend these deletion and retention protocols to an overarching data minimization rule that makes it 'an unfair trade practice to collect, use, transfer, or retain personal data beyond what is reasonably necessary and proportionate to the primary purpose for which it was collected, consistent with consumer expectations and the context in which the data was collected.'" The Commission agrees that data minimization is a crucial data security principle and is committed to utilizing its available enforcement mechanisms to their fullest extent. Moreover, the Commission has taken recent action to ensure companies prioritize deleting data when it is no longer in use. *See In the Matter of Drizly, Inc.* (Oct. 24, 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf.

Your comment also asks the Commission to strengthen regulations regarding personal data sharing with third parties due to the heightened risks associated with such sharing. As you note, the proposed order requires Blackbaud to "select and retain service providers capable of safeguarding covered information, along with contractual requirements for those providers to implement and maintain adequate safeguards." The proposed order also specifically mandates technical requirements for Blackbaud's employees, contractors, and third parties to secure any accounts with access to Blackbaud's information technology infrastructure, requiring the use of strong, unique passwords and preventing password reuse. While the proposed order contains strong requirements that address the concern you raise, with respect to the regulatory landscape, the Commission will take your comments under consideration as it reviews existing rules within its jurisdiction or proposes new regulations.

Finally, your comment suggests that the Commission articulate an expectation of enhanced protection for donor privacy in the proposed consent order. The proposed order provides express requirements and safeguards aimed at protecting the privacy of all consumers, including donors. For example, the mandated information security program protects the security, confidentiality, and integrity of Covered Information, which includes information about individuals, such as: first and last name, home address, email address, telephone number, drivers license, date of birth, or financial account information. Therefore, the Commission believes that the proposed order appropriately protects the information you identify as sensitive.

The Commission believes the proposed order offers substantial protections to consumers. The Commission has placed your comment on the public record, pursuant to Rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would best be served by issuing the Decision and Order in the

above-titled proceeding in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. Thank you again for your comment.

By direction of the Commission, Commissioner Ferguson not participating and Commissioner Holyoak recused.

April J. Tabor
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

May 17, 2024

Anonymous

Re: *In the Matter of Blackbaud, Inc.*, File No. 2023181

Dear Anonymous:

Thank you for your comment regarding the Federal Trade Commission's ("FTC") proposed consent agreement in the above-titled proceeding against Blackbaud, Inc. ("Blackbaud").

The complaint in this matter alleges that Blackbaud engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges that Blackbaud: (1) failed to employ reasonable information security practices to protect consumers' personal information; (2) failed to implement and enforce reasonable data retention practices; (3) failed to accurately communicate about the breach in its initial notification to customers; (4) misrepresented that it used appropriate safeguards to protect consumers' personal information; and (5) misrepresented the scope of the breach by stating that consumers' personal information had not been impacted by the breach in its initial notification.

Your comment calls on the Commission to hold Blackbaud accountable for its data security failures. The proposed order is specifically designed to address the misconduct alleged in the complaint and help ensure that Blackbaud will protect consumers' personal information moving forward. For instance, the proposed order prohibits Blackbaud from making misrepresentations about its data security and privacy policies. In addition, the proposed order requires Blackbaud to develop a comprehensive information security program, enact a data retention schedule, and notify the FTC if it experiences a future data breach that it would otherwise be required to report to any other local, state, or federal agency. The Commission agrees that accountability is important. For this reason, Blackbaud will be subject to independent, third-party assessments of its information security program and could face substantial civil penalties should it fail to comply with any obligations under the proposed order.

Your comment also raises concern regarding Blackbaud's lack of protection for consumers' personal information, particularly financial and medical information. The Commission is committed to protecting consumer data privacy and security and has included robust requirements in the proposed order. For example, the proposed order requires Blackbaud to encrypt fields in Blackbaud's products that are designed to store certain personal information, such as Social Security numbers; passport numbers; tax ID information; driver licenses; medical information associated with a consumer; and credit card, bank account, and debit card information. In response to the safety and identity theft concerns you raised in your comment, consider contacting your local authorities and state attorney general's office for assistance. For

additional information regarding identity theft, please visit the Commission's consumer identity theft resource page at https://consumer.ftc.gov/features/identity-theft.

The Commission believes the proposed order offers significant protections to consumers. For additional information on the settlement, please visit the Commission's business blog at https://www.ftc.gov/business-guidance/blog/2024/01/ftc-says-blackbauds-lax-security-allowed-hacker-steal-sensitive-data-thats-just-beginning-story.

The Commission has placed your comment on the public record, pursuant to Rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would best be served by issuing the Decision and Order in the above-titled proceeding in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. Thank you again for your comment.

By direction of the Commission, Commissioner Ferguson not participating and Commissioner Holyoak recused.

April J. Tabor
Secretary