UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 11165 / March 9, 2023

SECURITIES EXCHANGE ACT OF 1934
Release No. 97098 / March 9, 2023

ADMINISTRATIVE PROCEEDING
File No. 3-21339

In the Matter of

BLACKBAUD, INC.,

Respondent.

ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 ("Securities Act") and Section 21C of the Securities Exchange Act of 1934 ("Exchange Act"), against Blackbaud, Inc. ("Blackbaud" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds that:

Summary

1. This matter concerns materially misleading disclosures by Blackbaud regarding a ransomware attack that resulted in the unauthorized access and exfiltration of sensitive customer information. Blackbaud provides software that non-profit organizations use to manage data about their donors, including identifying information, donation history, and financial information. On May 14, 2020, Blackbaud discovered the attack, and the company's subsequent investigation indicated the attack resulted in the unauthorized access and exfiltration of over a million files concerning over 13,000, or roughly a quarter, of the company's customers.

2. On July 16, 2020, Blackbaud announced the incident on the company's website and notified the impacted customers. In the website post and notices, the company indicated that the attacker did not access any donor bank account information or social security numbers. Within days of these statements, however, the company's technology and customer relations personnel learned that these claims with respect to bank account information and social security numbers were erroneous. Nevertheless, on August 4, 2020, the company filed a Form 10-Q that discussed the incident, but omitted this material information about the scope of the attack, and misleadingly characterized the risk of exfiltration of such sensitive donor information as hypothetical. At the end of September 2020, the company disclosed for the first time that the attacker had, in fact, accessed unencrypted donor bank account information and social security numbers for certain of the impacted customers. The company also failed to maintain disclosure controls and procedures as defined in Exchange Act Rule 13a-15(e).

3. Based on the foregoing conduct, and the conduct described herein below, Blackbaud violated Sections 17(a)(2) and (3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-13, and 13a-15(a) thereunder.

Respondent

4. Blackbaud, Inc., a Delaware corporation headquartered in Charleston, South Carolina, provides donor relationship management software to various non-profit organizations, including charities, higher education institutions, K-12 schools, healthcare organizations, religious organizations, and cultural organizations. Blackbaud's common stock is registered pursuant to Section 12(b) of the Exchange Act. Blackbaud's common stock trades on the NASDAQ.

Facts

May 14, 2020 Cybersecurity Incident

5. On May 14, 2020, Blackbaud's technology personnel detected unauthorized access to the company's systems, and determined the access may have begun as early as February 2020. The personnel found messages from the attacker in the company's system claiming to have

exfiltrated data concerning Blackbaud's customers, and subsequently demanding payment. Blackbaud's technology personnel conducted an investigation of the incident in consultation with a third-party cybersecurity firm. In addition, Blackbaud's cybersecurity personnel consulted with a third-party vendor to engage in communications with the attacker, and ultimately coordinate payment of a ransom in exchange for the attacker's promise to delete the exfiltrated data.

6. By July 16, 2020, Blackbaud understood from the information available to it that the attacker exfiltrated at least a million files. The company's technology personnel analyzed the exfiltrated file names to identify which products and customers were impacted. The company did not analyze the content of any of the exfiltrated files, and Blackbaud did not direct any of its third party vendors to do so. Based on the file name review, the company's technology personnel identified over 13,000 impacted customers and multiple impacted products, including various versions of the company's donor relationship software.

July 16, 2020 Customer Notices and Website Post

7. On July 16, 2020, the company announced the incident for the first time on its website. The company also sent notices about the incident to the impacted customers. In both the customer notices and website post, the company stated "[t]he cybercriminal did not access . . . bank account information, or social security numbers."

8. By the end of July 2020, company personnel learned that the attacker had, in fact, accessed donor bank account information and social security numbers in an unencrypted form for a number of the impacted customers.

9. During the days following the notices and website post, Blackbaud received over a thousand communications from customers regarding the incident. A number of customers raised concerns that they had uploaded sensitive donor data—including social security numbers and bank account information—to fields that were not otherwise encrypted, or that they had included such information in attachments that were uploaded to Blackbaud's products and not encrypted.

10. These customer concerns were prevalent enough that by July 21, 2020, five days after the website post and notices, the company's personnel had developed a script for customer service personnel that acknowledged that certain attachments and fields potentially used to store social security numbers and bank account information were, in fact, not encrypted.

11. As a result of these customer inquiries, Blackbaud's personnel conducted further analysis of the potentially impacted products, and confirmed that certain donor bank account information and social security numbers had been accessed and exfiltrated by the attacker in an unencrypted format, contrary to the claims in the company's July 16, 2020 website post and notices. Although the company's personnel were aware of the unauthorized access and exfiltration of donor bank account numbers and social security numbers by the end of July 2020, the personnel with this information about the broader scope of the impacted data did not communicate this to Blackbaud's senior management responsible for disclosures, and the company did not have policies or procedures in place designed to ensure they do so.

August 4, 2020 Form 10-Q

12. On August 4, 2020, Blackbaud filed its Form 10-Q for the second fiscal quarter of 2020.

13. In the days preceding the Form 10-Q filing, between July 29, 2020, and July 30, 2020, the company met with analysts and held its quarterly earnings call, during which analysts asked several questions about the cybersecurity incident, including concerning the nature of the data impacted, which the company did not answer.

14. In Blackbaud's Form 10-Q filed on August 4, 2020, however, the company included a discussion about the scope of the incident, stating only that "the cybercriminal removed a copy of a subset of data." In that discussion, the company made no reference to the attacker removing any sensitive donor data, and in particular made no mention of the exfiltration of donor social security numbers and bank account numbers. This statement omitted the material fact that a number of customers had unencrypted bank account and social security numbers exfiltrated, in contrast to the company's unequivocal, and ultimately erroneous claims in the July 16, 2020 website post and customer notices.

15. Moreover, in the company's discussion of its cybersecurity risks in the Form 10-Q, the company stated, "A compromise of our data security that results in ***customer or donor personal*** or payment card data being obtained by unauthorized persons ***could*** adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties." (Emphasis added). This statement omitted the material fact that such customer or donor personal data was exfiltrated by the attacker, which entailed that the risks of such an attack on the company's business were no longer hypothetical.

16. Blackbaud's omissions of material facts about the scope of the incident and the company's cybersecurity risks in the August 4, 2020 Form 10-Q rendered the statements about the incident misleading because they perpetuated the false impression, started with the company's earlier website post and customer notices, that the incident did not result in the attacker accessing highly sensitive donor data—data at the core of the company's business as a service provider helping institutions manage donor relationships—when in fact the company's personnel learned before August 4, 2020 that such data had been accessed and exfiltrated by the attacker.

September 29, 2020 Form 8-K

17. On September 29, 2020, Blackbaud furnished a Form 8-K concerning the incident. The company acknowledged for the first time that "the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords." At or around that time, the company also sent supplemental notices to customers that Blackbaud believed had such sensitive donor information accessed and exfiltrated.

18. During the relevant period, Blackbaud offered and sold stock to its employees through an Equity and Incentive Compensation Plan for which a Form S-8 was filed with the Commission on June 16, 2016.

Blackbaud's Disclosure Control and Procedures Failures

19. Exchange Act Rule 13a-15(a) requires issuers such as Blackbaud to "maintain disclosure controls and procedures (as defined in paragraph (e) of this section)." Paragraph (e) defines disclosure controls and procedures to include, among other things, "controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the [Exchange] Act . . . is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms." Under the rule, "[d]isclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the [Exchange] Act is accumulated and communicated to the issuer's management . . . as appropriate to allow timely decisions regarding required disclosure."

20. Blackbaud's primary business includes providing software that allows its customers to manage data, including sensitive financial and personal data, concerning their donors. Nevertheless, during the relevant time frame, Blackbaud did not have disclosure controls and procedures related to the disclosure of cybersecurity risks or incidents, including incidents involving the exposure of sensitive donor information.

21. As described above, certain of the company's technical and customer response personnel learned shortly after the July 16, 2020 customer notices and website post that, contrary to the representations therein, the attacker accessed and exfiltrated sensitive donor information including banking information and social security numbers that certain customers had included in unencrypted attachments and fields.

22. Nevertheless, the company's senior management responsible for the company's disclosures were not made aware of these facts prior to the company filing its Form 10-Q on August 4, 2020, or indeed until several weeks later, nor were there controls or procedures designed to ensure that such information was communicated to senior management. The company did not have controls or procedures designed to ensure that information relevant to cybersecurity incidents and risks were communicated to the company's senior management and other disclosure personnel. As a result, relevant information related to the incident was never assessed from a disclosure perspective.

Violations

23. As a result of the conduct described above, Blackbaud violated Sections 17(a)(2) and (3) of the Securities Act, which prohibit any person from directly or indirectly obtaining money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading, or engaging in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser, in the offer or sale of securities. A violation of these provisions does not require scienter and may rest on a finding of negligence. *See Aaron v. SEC*, 446 U.S. 680, 701-02 (1980).

24. In addition, Blackbaud violated Section 13(a) of the Exchange Act and Rule 13a-13 thereunder, which require issuers of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission quarterly reports in conformity with the Commission's rules and regulations. Blackbaud also violated Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in quarterly reports filed with the Commission any material information necessary to make the required statements in the filing not misleading.

25. In addition, Blackbaud violated Exchange Act Rule 13a-15(a), which requires most issuers such as Blackbaud with a security registered pursuant to Section 12 of the Exchange Act to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent Blackbaud's Offer.

Accordingly, it is hereby ORDERED that**:**

A. Pursuant to Section 8A of the Securities Act and Section 21C of the Exchange Act, Respondent cease and desist from committing or causing any violations and any future violations of Sections 17(a)(2) and (3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-13, and 13a-15 thereunder.

B. Respondent shall, within 14 days of the entry of this Order, pay a civil money penalty in the amount of $3,000,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard

Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying Blackbaud as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to David Hirsch, Division of Enforcement, Securities and Exchange Commission, 100 F Street, N.E., Washington, District of Columbia 20549.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary