2023181

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

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

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. ÑSummary of the Case

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

Blackbaud's Business Practices

aud provides a variety of data services and financial, fundraising, and strative software services to its customers, more than 45,000 companies, fits, foundations, educational institutions, healthcare organizations, and individual ners throughout the U.S. and abroad. It maintains a wide variety of consumers' al 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 rema771.15 3.76 04ii 3 (a771.1 3.76eti)-2 (c(3 (cti)-2 (d)-4 (es)]TJ-0.003 Tc 0.0

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

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

[illegible] 502 Tc -0.002 Tw T*aTc -0.002

---

data security events; and perform regular assessments as to the

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