ROB BONTA
Attorney General of California
KATHLEEN BOERGERS
Acting Senior Assistant Attorney General
NICKLAS AKERS
Senior Assistant Attorney General
KARLI EISENBERG
STACEY SCHESSER
Supervising Deputy Attorneys General
YEN P. NGUYEN (SBN 239095)
DARCIE TILLY (SBN 239715)
Deputy Attorneys General
600 West Broadway, Suite 1800
San Diego, CA 92101
P.O. Box 85266
San Diego, CA 92186-5266
Telephone: (619) 738-9559
E-mail: Darcie.Tilly@doj.ca.gov

Attorneys for Plaintiff, the People of the State of California

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

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN DIEGO

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, v. BLACKBAUD, INC., a corporation, Defendant.	Case No. **COMPLAINT FOR INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF** (Bus. & Prof. Code, §§ 17200 et seq., 17500 et seq.)

The People of the State of California (People), by and through Rob Bonta, Attorney General of the State of California, bring this action against Defendant Blackbaud, Inc. (Defendant) for violations of California's Unfair Competition Law, Business and Professions Code section 17200 et seq., and False Advertising Law, Business and Professions Code section 17500 et seq. The People allege the following facts based on investigation, information, or belief:

INTRODUCTION

1. Blackbaud is a publicly traded software-as-a-service company for not-for-profit companies, foundations, education institutions, healthcare organizations, and others. It offers

solutions to help its customers in securing resources, managing their operations, delivering their programs, and measuring their impact. Blackbaud claims that at the end of 2019 it had over 45,000 customers located in over 100 countries.

2. Blackbaud maintains, among other things, names, Social Security numbers, bank account information, and medical information of California residents for Blackbaud customers who store such personal information in connection with their use of Blackbaud's products and services.

3. Blackbaud, however, failed to use appropriate information security practices to protect consumers' personal information resulting in a 2020 data breach in which a threat actor accessed Blackbaud's customer databases and stole personal information relating to California residents. Blackbaud compounded the impact of the breach when it made unfair, deceptive, untrue, and misleading statements about its security practices at the time of the breach and in downplaying the severity of the data breach.

PARTIES

4. Plaintiff is the People of the State of California. The People bring this action by and through Rob Bonta, Attorney General, who is authorized by Business and Professions Code sections 17204 and 17206 to bring actions to enforce the Unfair Competition Law, and Business and Professions Code section 17536 to bring actions to enforce the False Advertising Law.

5. Defendant Blackbaud is a Delaware corporation with its principal office located at 65 Fairchild Street, Charleston, South Carolina 29492.

JURISDICTION AND VENUE

6. The Court has jurisdiction over the subject matter of this action, jurisdiction over the parties to this action, and venue is proper in this Court.

7. Blackbaud has transacted business within the State of California, including the County of San Diego, at all times relevant to this complaint. The violations of law described herein occurred in the County of San Diego, and elsewhere in the State of California.

FACTS

I. BLACKBAUD'S PRE-BREACH SECURITY REPRESENTATIONS

8. At times relevant to this action, Blackbaud represented to its customers that its "security, privacy, and risk-management teams work every day to ensure the safety of [its customers'] data by adhering to industry standard practices, conducting ongoing risk assessments, aggressively testing the security of our products, and continually assessing our infrastructure."

9. At times relevant to this action, Blackbaud represented in its privacy policy that "[w]e protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons."

II. BLACKBAUD DATA BREACH

10. On May 14, 2020, Blackbaud's technology personnel detected unauthorized access to the company's systems. The threat actor who gained unauthorized access to Blackbaud's systems threatened to publish several hundred terabytes of Blackbaud's customers' sensitive data if a ransom was not paid. Blackbaud thereafter paid the threat actor a ransom in exchange for the threat actor's promise to destroy this data.

11. Following an investigation by Blackbaud, the company determined the threat actor had been able to access and exfiltrate personal data belonging to over 13,000 Blackbaud customers, including customers in California. The consumer data accessed and exfiltrated included Social Security numbers, bank account information, and medical information.

12. Reasonable security procedures and practices could have protected the personal information of California residents from unauthorized access or disclosure.

13. For example, the threat actor was able to gain entry to Blackbaud's system by using a Blackbaud customer's compromised login and password to access the customer's Blackbaud virtual desktop environment. Blackbaud did not implement appropriate password controls, such as mandating all customers accessing sensitive environments rotate passwords and avoid default, weak, or identical passwords. Blackbaud also failed to mandate authentication protocols, like multi-factor authentication, as a separate layer of security to protect its system from unauthorized entry.

14. Prior to the data breach, Blackbaud also had additional vulnerabilities, including failing to implement appropriate network segmentation. Because of these vulnerabilities and the lack of appropriate network segmentation, the threat actor was able to escape the customer virtual desktop environment, escalate his access to that of an administrator, and then move across multiple Blackbaud-hosted environments. The threat actor was consequently able to access data that, had appropriate measures been put in place, otherwise would have been inaccessible to him.

15. Blackbaud also failed to adequately prevent its customers from storing personal information of consumers, including Californians, in unencrypted fields, even though these fields did not include the degree of security necessary for the storage of information of that nature. Blackbaud's failure includes not implementing an adequate inventory process, such as through the use of a sufficiently robust commercially-available automated tool, to detect and prevent personal information of consumers from being located outside designated, encrypted, locations. This resulted in the threat actor being able to access personal information of California residents.

16. Most troubling, Blackbaud stored data belonging to Blackbaud's customers for years longer than necessary. This data contained unencrypted personal information of California residents. Had Blackbaud implemented data minimization principles or appropriate retention policies, it could have mitigated the threat actor's exfiltration of data.

17. Finally, Blackbaud did not implement appropriate threat and intrusion detection processes, which allowed the threat actor to move throughout its systems and exfiltrate data undetected from early February 2020 until the threat actor was detected in mid-May 2020.

III. BLACKBAUD'S STATEMENTS ABOUT THE DATA BREACH

18. On July 16, 2020, Blackbaud announced the incident on its website and notified impacted customers by email. In both, Blackbaud stated the threat actor did not access bank account information or Social Security numbers. Blackbaud reiterated this representation in its subsequent communications and conversations with customers.

19. Blackbaud's statements were false, which Blackbaud knew or should have known at the time it made the representations. In fact, by early August 2020 Blackbaud knew consumer bank account information and Social Security numbers were exfiltrated by the threat actor. Yet,

Blackbaud continued to make representations that the threat actor did not access bank account information or Social Security numbers. It was not until late September 2020 that Blackbaud sent out supplemental notifications to its customers and the public admitting and alerting them to the fact this personal information was compromised.

20. Additionally, in its initial July 16, 2020, announcement on its website and subsequent communications with customers, Blackbaud repeated its pre-breach statement that it "follow[s] industry-standard best practices[.]"

21. Again, Blackbaud's statements were false, which Blackbaud knew or should have known at the time it made the representations. Blackbaud lacked reasonable security procedures and practices to protect the personal information of California residents from unauthorized access or disclosure.

FIRST CAUSE OF ACTION

VIOLATIONS OF THE UNFAIR COMPETITION LAW (BUSINESS AND PROFESSIONS CODE SECTION 17200 ET SEQ.)

22. The People re-allege and incorporate by reference each of the paragraphs above as though fully set forth herein.

23. Blackbaud engaged in unlawful, unfair or fraudulent acts and practices and unfair, deceptive, untrue or misleading advertising and acts prohibited by Business and Professions Code section 17500, which constitute unfair competition within the meaning of Section 17200 of the Business and Professions Code.

24. Blackbaud's acts or practices that violate Section 17200 of the Business and Professions Code include, but are not limited to, failing to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure in violation of Civil Code section 1798.81.5, subdivision (b). This provision requires a business that owns or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. (Cal. Civ. Code

§ 1798.81.5, subd. (b).) The statute defines personal information to include name and Social Security number, financial information, as well as "medical information[.]" (*Id*. § 1798.81.5, subds. (d)(1)(A)(i), (iii) & (iv), (d)(2).)

25. Blackbaud's acts or practices that violate Section 17200 of the Business and Professions Code also include, but are not limited to, making false, deceptive, or misleading statements regarding its security measures in place at the time of the data breach and its statements regarding the data breach.

SECOND CAUSE OF ACTION

VIOLATIONS OF THE FALSE ADVERTISING LAW (BUSINESS AND PROFESSIONS CODE SECTION 17500 ET SEQ.)

26. The People re-allege and incorporate by reference each of the paragraphs above as though fully set forth herein.

27. Blackbaud engaged in acts or practices that constitute violations of Business and Professions Code section 17500 by making or disseminating, or causing to be made or disseminated, untrue or misleading statements with the intent to induce members of the public to use Blackbaud's services or products when Blackbaud knew, or by the exercise of reasonable care should have known, that the statements were untrue or misleading.

28. Blackbaud's untrue or misleading statements include, but are not limited to, its statements regarding its security measures in place at the time of the data breach and its statements regarding the data breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

1. Under Business and Professions Code sections 17203 and 17535, that Blackbaud, its affiliates, subsidiaries, successors and assigns, its officers and employees, and all persons who act in concert with Blackbaud, be permanently enjoined from committing any unlawful, unfair, or fraudulent acts of unfair competition in violation of Business and Professions Code section 17200 and false advertising in violation of Business and Professions Code section 17500 as alleged in this Complaint;

2. That the Court assess a civil penalty of $2,500 against Blackbaud for each violation of Business and Professions Code section 17200 in an amount according to proof, under the authority of Business and Professions Code section 17206;

3. That the Court assess a civil penalty of $2,500 against Blackbaud for each violation of Business and Professions Code section 17500 in an amount according to proof, under the authority of Business and Professions Code section 17536;

4. That the People of the State of California recover its costs of suit, including costs of its investigation; and

5. For such other and further relief that the Court determines to be just and proper.

Dated: June 12, 2024

Respectfully Submitted,

ROB BONTA
Attorney General of California

/s/ Darcie Tilly
BY: DARCIE TILLY
Deputy Attorney General
Attorney for Plaintiff