UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

PAM ARTHUR and DOROTHY KAMM on behalf of themselves and all others similarly situated,	:	
Plaintiffs,	:	**CIVIL ACTION NO.:**
v.	:	
BLACKBAUD, INC.,	:	
Defendant.	:	

CLASS ACTION COMPLAINT

1. Plaintiffs, Pam Arthur and Dorothy Kamm, individually and on behalf of all others similarly situated, bring this action against Defendant Blackbaud, Inc. ("Blackbaud" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

2. This class action arises out of the May of 2020, ransomware attack and data breach ("Data Breach") of several schools, healthcare, non-profit companies, and other organizations (collectively "Clients") whose data and servers were managed, maintained, and secured by Blackbaud. The Clients' data and servers contained identifying, sensitive, and personal data from students, patients, donors, and other individual users, including Plaintiffs'. As a result of the Data Breach, Plaintiffs and thousands of other Class Member users suffered

ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. Additionally, Plaintiffs and Class Members' sensitive personal information—which was entrusted to Defendant, its officials and agents—was compromised and unlawfully accessed due to the Data Breach. Information compromised in the Data Breach included a copy of a subset of information retained by Blackbaud, including name(s), addresses, phone numbers, and other personal information. True and accurate copies of the notices of data breach mailed to Plaintiffs ("Notice") is attached hereto, and Defendant's exemplar Notice is available on its website.[1] Contrary to the representations in the Notice regarding the type of accessed information, it is believed based on statements by Defendant's Clients directing Class Members to monitor suspicious activity of their credit and accounts, that Social Security Numbers, credit card numbers, bank account numbers, and additional personally identifiable information (collectively "Private Information") may also have been compromised.

3. Plaintiffs bring this class action lawsuit on behalf of themselves and those similarly situated, in order to, (1) address Defendant's inadequate safeguarding of Class Members' Private Information, which Defendant managed, maintained, and secured; (2) for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third-party; (3) for failing to identify all information that was accessed; and (4) for failing to provide Plaintiffs and Class Members with any redress for the Data Breach.

4. Defendant maintained and secured the Private Information in a reckless manner, including, *inter alia*, failing to safeguard against ransomware attacks. In particular, the Private

[1] https://www.blackbaud.com/securityincident (Last Accessed August 12, 2020).

Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

5. In addition, Defendant and their employees failed to properly monitor the computer network and systems that housed the Private Information; failed to implement appropriate policies to ensure secure communications; and failed to properly train employees regarding ransomware attacks. Had Defendant properly monitored their network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Blackbaud has announced it has "already implemented changes to prevent this specific issue from happening again."[2] In other words, had these changes been in place previously, this incident would not have happened and Plaintiffs and Class Members' Private Information would not have been accessed.

6. Plaintiffs and Class Members' identities and Private Information are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained was in the hands of data thieves. Defendant cannot reasonably maintain that the data thieves destroyed the subset copy simply because Defendant paid the ransom and the data thieves confirmed the copy was destroyed. In fact, the notices advise the affected individuals to monitor their own credit, suspicious account activity, and notify the school or non-profit of suspicious activity related to his or her credit. Despite this, Defendant has not offered any manner of redress, including, *inter alia*, credit monitoring.

[2] https://www.blackbaud.com/securityincident (Last Accessed August 12, 2020).

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using Plaintiffs and Class Members' names to obtain medical services, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names, but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members, at their own cost, must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Consequently, Plaintiffs and Class Members will also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By their Complaint, Plaintiffs seeks to remedy these harms on behalf of themselves and all similarly-situated individuals, whose Private Information was accessed during the Data Breach.

11. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiffs brings this action against Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) violation of privacy, (iii) negligence *per se*, (iv) breach of express contract, and (v) breach of implied contract.

PARTIES

13. Plaintiff Pam Arthur is a resident and citizen of Stuart, Martin County, Florida.

14. Plaintiff Dorothy Kamm is a resident and citizen of Port St. Lucie, St. Lucie County. Florida.

15. Defendant Blackbaud is a Delaware corporation with its principal place of business located on Daniel Island, Charleston County, South Carolina.

16. Defendant manages, maintains, and provides cybersecurity for the data obtained by its clients who are, *inter alia*, schools and non-profit companies, including Bread for the World and Planned Parenthood, which maintained Plaintiffs' Private Information.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

18. This Court has personal jurisdiction over this action because Defendant holds its principal place of business in this District has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.