Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of Blackbaud, Inc.*, File No. 2023181**

The Federal Trade Commission (the "Commission") has accepted, subject to final approval, an agreement containing consent order from Blackbaud, Inc. ("Respondent" or "Blackbaud").

The proposed consent order ("Proposed Order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

Blackbaud is a publicly traded South Carolina corporation that provides a variety of data services and financial, fundraising, and administrative software solutions to over 45,000 companies, nonprofits, foundations, educational institutions, healthcare organizations, and individual customers throughout the U.S. and abroad. Blackbaud maintains the personal information of millions of U.S. consumers that have donor, student, patient, and other relationships with Blackbaud's customers.

According to the FTC's Complaint, despite representing that it would protect consumers' data from unauthorized access through a variety of safeguards, from February through May 2020, Blackbaud's networks suffered a data breach from an attacker that exfiltrated data from thousands of Blackbaud customers. This data comprised of millions of consumers' personal information, including, in some cases, sensitive information including social security numbers and financial information. Adding to the scope and severity of the breach was Blackbaud's indefinite retention of customer backup files, which impacted additional current, prospective, and former customers, whose consumer data would not have otherwise been impacted by the data breach. And when Blackbaud informed customers of the breach in July 2020, its initial breach notification statement inaccurately stated that the hacker had not stolen sensitive consumer data. Blackbaud did not correct this information until October 2020, despite knowing it was inaccurate only a couple of weeks after the initial breach notification.

The Commission's proposed five-count complaint alleges that Respondent violated Section 5(a) of the FTC Act by (1) failing to employ reasonable information security practices to protect consumers' personal information; (2) failing to implement and enforce reasonable data retention practices; (3) failing to accurately communicate about the breach in its initial breach notification; (4) misrepresenting that it used appropriate safeguards to protect consumers' personal information; and (5) misrepresenting the scope of the breach by stating that consumers' personal information had not been impacted by the breach in its initial notification. With respect to the first count, the proposed complaint alleges that Respondent:

- failed to implement appropriate password controls, which resulted in employees often using default, weak or identical passwords;

- failed to apply adequate multifactor authentication for both employees and customers to protect sensitive consumer information;

- failed to prevent data theft by (1) monitoring for unauthorized attempts to transfer or exfiltrate consumers' personal information from its networks; (2) continuously logging and monitoring its systems and assets to identify data security events; and (3) performing regular assessments as to the effectiveness of protection measures;

- failed to implement and enforce appropriate data retention schedules and deletion practices for the vast amounts of consumers' personal information stored on its network;

- failed to patch outdated software and systems in a timely manner;

- failed to 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;

- failed to implement appropriate firewall controls; and

- failed to implement appropriate network segmentation to prevent attackers from moving freely across its networks and databases.

The proposed complaint alleges that Respondent could have addressed each of these failures by implementing readily available and relatively low-cost security measures.

With respect to the second count, the proposed complaint alleges that Respondent failed to implement and enforce reasonable data retention practices for sensitive consumer data maintained by its customers on its network.

With respect to the third count, the proposed complaint alleges that Respondent failed to accurately communicate the scope and severity of the breach in its initial notification to consumers.

The proposed complaint alleges that, with respect to counts one, two, and three, that Respondent's failures caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

With respect the fourth count, the proposed complaint alleges that, at various times, Respondent claimed that is used appropriate safeguards to protect consumers' personal information. The proposed complaint alleges that, in reality, and as noted above, Respondent failed to implement reasonable measures to protect consumer's personal information. Such representations were deceptive under Section 5 of the FTC Act.

With respect to the fifth count, the proposed complaint alleges that, in its initial breach notification, Respondent claimed that consumers' personal information had not been subject to the breach. The proposed complaint alleges that, in reality, and as noted above, consumers' personal information had been exfiltrated by the attacker in the breach. Such representations were, therefore, deceptive under Section 5 of the FTC Act.

Summary of the Proposed Order with Respondent

The Proposed Order contains injunctive relief designed to prevent Respondent from engaging in the same or similar acts or practices in the future.

Part I prohibits Respondent from misrepresenting the extent (1) to which it maintains, uses, deletes or disclosed consumers' personal information; (2) to which it protects the privacy, security, availability, confidentiality, or integrity of consumers' personal information; or (3) of any future data security incident or unauthorized disclosure of consumers' personal information.

Part II requires Respondent to delete or destroy customer backup files containing consumers' personal information that are not being retained to provide its products or services and to refrain from maintaining consumers' personal information that is not necessary for the purposes for which it is maintained by Respondent.

Part III requires that Respondent document and adhere to a retention schedule for its customer backup files containing consumers' personal information, including the purposes for which it maintains such information, the business needs for its retention, and the timeframe for its deletion.

Part IV requires that Respondent establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, availability, confidentiality, and integrity of consumers' personal information.

Part V requires Respondent to obtain initial and biennial information security assessments by an independent, third-party professional for 20 years.

Part VI requires Respondent to disclose all material facts to the assessor required by **Part V** and prohibits Respondent from misrepresenting any fact material to the assessments required by **Part IV**.

Part VII requires Respondent to submit an annual certification from its Chief Information Security Officer that the company has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VIII requires Respondent to notify the Commission any time it notifies a federal, state, or local government that consumer personal information was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

Parts IX-XII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance.

Part XIII states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.