UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

Joint Statement of Chair Lina M. Khan,
Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya
In the Matter of Blackbaud, Inc.
Commission File No. 202-3181

February 1, 2024

Today the FTC brings an enforcement action against Blackbaud for a series of unfair and deceptive data security practices. Blackbaud provides backend services for a variety of entities, ranging from businesses and nonprofits to schools and healthcare organizations. As noted in the FTC's complaint, Blackbaud in 2020 was struck by a data breach that exposed the personal data of millions of Americans. The FTC charges that Blackbaud's reckless data retention practices rendered its security failures much more costly: by hoarding reams of data that it did not reasonably need, Blackbaud's breach exposed far more data. Moreover, Blackbaud's notification alerting victims of the breach included false statements, which Blackbaud did not correct until months later—and months after it knew the statements were false.

The FTC's complaint alleges that Blackbaud's practices violated Section 5's prohibition on unfair or deceptive practices. The complaint marks a new step forward by alleging standalone unfairness counts for (a) failure to implement and enforce reasonable data retention practices (Count II) and (b) failure to accurately communicate the scope and severity of the breach in its notification to consumers (Count III).[1] Blackbaud's data retention failures exacerbated the harms of its data security failures because Blackbaud had failed to delete data it no longer needed. This action illustrates how indefinite retention of consumer data, which can lure hackers and magnify the harms stemming from a breach, is independently a prohibited unfair practice under the FTC Act. Similarly, Blackbaud's failure to accurately convey the scope and severity of the breach kept victims in the dark and delayed them from taking protective actions, making a bad situation even worse.

Today's action builds on a series of cases that have made clear that maintaining a data retention and deletion schedule is a critical part of protecting consumers' data security.[2] The