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

[1] Complaint, *In re Blackbaud, Inc.*, FTC Matter No. 202 3181 (Feb. 1, 2024) ¶¶ 29-34, https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.

[2] *See, e.g.*, Press Release, Fed. Trade Comm'n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without; Press Release, Fed. Trade Comm'n, FTC Finalizes Order With Online Alcohol Marketplace For Security Failures That Exposed Personal Data of 2.5 Million People (Jan. 10, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-online-alcohol-marketplace-security-failures-exposed-personal-data-25-million; Press Release, Fed. Trade Comm'n, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers (Oct. 31, 2022); Press Release, Fed.

Commission has also made clear that efforts to downplay the extent or severity of a data breach run afoul of the law.[3]

We are grateful to the Division of Privacy and Identity Protection for their excellent work, which enables us to continue making key strides in protecting people's data. As businesses face fresh incentives to hoard data to train AI models,[4] protecting Americans from unlawful data practices will be especially critical.

***

Trade Comm'n, FTC Takes Action Against Global Tel*Link Corp. for Failing to Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-takes-action-against-global-tellink-corp-failing-adequately-secure-data-notify-consumers-after. *See also* FTC Technology Blog, Security Principles: Addressing Underlying Causes of Risk in Complex Systems (Feb. 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems.

[3] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover. *See also* FTC Technology Blog, Security Beyond Prevention: The Importance of Effective Breach Disclosures (May 20, 2022), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/security-beyond-prevention-importance-effective-breach-disclosures.

[4] Press Release, Fed. Trade Comm'n, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Request (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.