epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 14, 2024

Chair Lina M. Khan
Commissioner Rebecca Kelly Slaughter
Commissioner Alvaro Bedoya
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan and Commissioners Slaughter and Bedoya,

In a notice released in 2024, the Federal Trade Commission (FTC) announced a proposed consent order with Blackbaud, Inc.[1] This order is in response to alleged violations by Blackbaud of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. §45(a), which prohibits unfair and/or deceptive acts or practices, in or affecting commerce.[2] The proposed consent order stems from the FTC's complaint, which accuses Blackbaud of breaching the FTC Act by failing to implement adequate information security measures to safeguard consumers' personal data.[3] This failure resulted in a cyberattack that compromised Blackbaud's customer databases, leading to the theft of personal information belonging to millions of U.S. consumers.[4]

The Electronic Privacy Information Center (EPIC) submits this letter to applaud the FTC's efforts in this matter and to provide recommendations to strengthen the proposed order (and others like it in future cases concerning breaches of data privacy).[5] EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC routinely files comments in response to proposed FTC consent orders and complaints regarding business practices that violate privacy rights.[6]

---

[1] Blackbaud, Inc., Decision & Proposed Order, In the Matter of Blackbaud, Inc., FTC File No. 202-3181 (2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-D%26O.pdf [hereinafter "Proposed Order"].
[2] Blackbaud, Inc., Complaint, *In the Matter of Blackbaud, Inc.*, FTC File No. 202-3181 (2023), *https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf* at ¶ 2 [hereinafter Complaint].
[3] *Id*. at ¶ 3.
[4] *Id*. at ¶ 3.
[5] EPIC Spring Intern Chloe Le contributed to the preparation of these comments.
[6] *See, e.g.*, EPIC, Comments of EPIC, Demand Progress, and EFF in re the Federal Trade Commission's Proposed Order & Settlement with X-Mode Social, Inc. (Feb. 20, 2024), https://epic.org/documents/comments-of-epic-demand-progress-and-eff-in-re-the-federal-trade-commissions-proposed-order-settlement-with-x-mode-social-inc/; EPIC, EPIC Commends FTC for Including Data Minimization & Data Rights in Chegg Settlement (Dec. 12, 2022), https://epic.org/epic-commends-ftc-for-including-data-minimization-data-rights-in-chegg-settlement/; EPIC, EPIC Applauds FTC SpyFone Ban, Urges Similar Remedies in Future Privacy Cases (Oct. 8, 2021), https://epic.org/epic-applauds-ftc-spyfone-ban-urges-similar-remedies-in-future-privacy-cases/.

EPIC commends the Commission for exercising its authority to investigate and take enforcement actions against companies like Blackbaud that have engaged in unfair and deceptive practices, particularly practices involving inadequate protection of personal information. Blackbaud's collection and storage of personal data encompasses a vast spectrum of employee records and consumer information. Millions of donors whose data was exposed likely had no choice in the fact that the nonprofits they supported entrusted Blackbaud with sensitive information such as religious affiliations, family backgrounds, dates of birth, income brackets, sexual orientations, and disabilities. Moreover, Blackbaud failed to safeguard Social Security numbers, financial account details, and other private information gathered from its employees. Despite assuring consumers of robust data security measures, Blackbaud's practices fell short, leading to a months-long breach by hackers compromising multiple Blackbaud-hosted environments. This included full names, ages, addresses, email addresses, medical records, and account credentials.[7]

EPIC supports the FTC's Consent Order. We are particularly encouraged by the order's data minimization mandate, third-party oversight requirements, and attention to underreporting. However, we urge the Commission to consider the chilling effect data security incidents like Blackbaud's can have on donations to nonprofits. The mishandling of personal data by donor management platforms may cause donors to fear their charitable giving will expose them to enhanced privacy risks, which could in turn impact the capacity of nonprofit organizations to achieve their important missions or even jeopardize their viability. As such, the Commission should hold vendors who would provide services to nonprofit organizations to at least the same baseline cybersecurity standards as other commercial actors, if not more rigorous standards. We re-iterate[8] what these standards should include at the end of this letter, drawing on the Commission's own past enforcement actions.

EPIC supports the proposed order's mandate to "[d]elete or destroy Respondent customer backup files containing Covered Information that is not being retained in connection with providing products or services to Respondent's customers."[9] Every piece of personal information collected and retained by an entity is inherently at risk of unauthorized access and use.[10] As a matter of hygiene, it is a best practice to promptly delete data after it is no longer necessary because data that does not exist cannot be stolen by hackers. Similarly, EPIC applauds the proposed order's detailed data retention limits, which require Blackbaud to create and publish a retention schedule on its website(s) outlining the purpose, business needs, and timeframe for deletion of customer backup files

[7] Complaint at ¶ 8.
[8] *See* EPIC, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem 181-216 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter "EPIC Commercial Surveillance Comment"].
[9] Proposed Order, *supra* note 1 at 6.
[10] *See* John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, (Jun. 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.

containing Covered Information, including databases for former and migrating customers.[11] As EPIC has consistently advocated, the Commission should extend these deletion and retention protocols to an overarching data minimization rule that makes it "an unfair trade practice to collect, use, transfer, or retain personal data beyond what is reasonably necessary and proportionate to the primary purpose for which it was collected, consistent with consumer expectations and the context in which the data was collected."[12] Establishing these foundational standards would not only afford meaningful protection for consumers' personal information but also furnish entities with clear directives on how to fortify consumer privacy.[13] This alignment of standards would ultimately reinforce a consumer trust and confidence in data handling practices across industries.

Furthermore, EPIC calls on the FTC to strengthen regulations regarding the sharing of personal data with third parties, recognizing the heightened risks to data security and privacy that such sharing entails. EPIC commends the proposed order's mandate that Blackbaud select and retain service providers capable of safeguarding covered information, along with contractual requirements for those providers to implement and maintain adequate safeguards.[14] As EPIC has previously stated, regulated entities must guard against incidents originating from access by third parties, even if the third party is not directly regulated.[15] This ensures that the security of covered information is maintained even when handled by third parties.

Additionally, EPIC supports the Commission emphasizing the harms that can result when companies report a breach but under-report its severity.[16] This is not the first time and it will not be the last time that a company fails to update customers with timely information about the risks a breach may pose to them. For example, personal genomics company 23andMe initially claimed that only 14,000 records were compromised in a 2023 breach.[17] Subsequently, 23andMe admitted that hackers had gained access to data on millions of users.[18] While we recognize that a breached company may be reporting to the best of its knowledge, an unreasonable delay in updating consumers when the

[11] Proposed Order.
[12] Davisson, *supra* note 10.
[13] John Davisson and Suzanne Bernstein, *Comments of EPIC in re the Federal Trade Commission's Proposed Order & Settlement With Chegg, Inc.*, EPIC (Dec. 12, 2022), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-chegg-inc/.
[14] Proposed Order at 8.
[15] *See, e.g.*, Comments of EPIC, In re Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations (RFI), ONCD-2023-0001 (Oct. 2023), https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/ [hereinafter "EPIC ONCD Comment"].
[16] Complaint at ¶ 12-15.
[17] *See* Addressing Data Security Concerns, 23andMe Blog (Dec. 5, 2023), https://blog.23andme.com/articles/addressing-data-security-concerns.
[18] *See* Emma Roth, *23andMe admits hackers accessed 6.9 million users' DNA Relatives data*, The Verge (Dec. 4, 2023), https://www.theverge.com/2023/12/4/23988050/23andme-hackers-accessed-user-data-confirmed.

company learns more is itself a deceptive and unfair practice. Consumers heavily rely on receiving timely and accurate information to assess the risks posed by a breach and to take necessary steps to safeguard their personal information. When companies fail to promptly disclose breaches or downplay their severity, consumers are left uninformed about the full extent of the threat to their privacy and security.[19] This issue is not an isolated incident but rather highlights a systemic problem of under-reporting or misreporting breaches in the industry.[20] Without robust enforcement measures and clear guidelines from regulatory bodies such as the FTC, companies may continue to prioritize their reputation or financial interests over the fundamental rights of their customers to privacy and security. In light of these concerns, EPIC hopes that the Commission's emphasis on the specific practice of underreporting the severity of breaches will serve as a powerful message to companies regarding their responsibilities in responding to such incidents. Accurate and timely reporting is essential not only for enabling affected individuals to take appropriate measures to mitigate potential harms, but also for upholding consumer trust and confidence in a company's commitment to safeguarding their data.

EPIC also respectfully requests that the FTC consider articulating an explanation of enhanced protection for donor privacy in its consent order. Donors may face social, professional, or legal repercussions, if their contributions are made public. This is particularly true in politically charged environments or when supporting controversial causes. For instance, individuals who donated to the Peachtree-Pine homeless shelter to oppose its closure for the construction of a fire and police station chose anonymity due to fears of backlash.[21] Donor privacy directly impacts participation rates in political and charitable activities; individuals may be hesitant to contribute if they fear their personal information will be disclosed without consent.[22] EPIC emphasizes the importance of robust confidentiality protocols to safeguard donor information, including names, contact details, contribution amounts, and other identifying information. Access to donor information should be restricted to authorized personnel only. Organizations must establish clear guidelines and protocols for accessing and handling donor data, ensuring it is used solely for intended purposes and not shared or disseminated without explicit consent, even in the event of a breach. Therefore, we urge

[19] *See* Report and Order, *In re Data Breach Reporting Requirements*, WC Dkt. No. 22-21 at ¶ 21 (Rel. Dec. 21, 2023), https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf.
[20] *See, e.g.*, Rebecca Pifer, *Scope of CommonSpirit data breach larger than initially disclosed*, Health Care Dive (Apr. 10, 2023), https://www.healthcaredive.com/news/scope-commonspirit-data-breach-larger/647198/; Eduard Kovasc, *Twitter Data Breach Bigger Than Initially Reported*, Security Week (Nov. 28, 2022), https://www.securityweek.com/twitter-data-breach-bigger-initially-reported/.
[21] *See* Sean Parnell, *The Legal and Political Landscape of Donor Privacy*, Philanthropy Roundtable (2017), https://www.philanthropyroundtable.org/magazine/spring-2017-the-legal-and-political-landscape-of-donor-privacy/.
[22] *See, e.g.*, Americans for Prosperity Found. v. Bonta, 141 S. Ct. 2373, 2388 (2021) ("The deterrent effect feared by these organizations is real and pervasive, even if their concerns are not shared by every single charity operating or raising funds in California.").

the FTC to consider these concerns and take appropriate action to protect donor privacy, such as articulating an expectation of enhanced protection for donor data in enforcement actions and regulations.

Finally, we applaud the consistency with which the FTC has taken companies to task for their deficient cybersecurity practices over the past decade or more,[23] and we urge the Commission to continue incorporating rigorous third-party audits and evaluations in future consent orders to deter inadequate cybersecurity and breach notification practices. The cybersecurity measures in the current order include that Blackbaud must implement and maintain an information security program,[24] data mapping,[25] damage mitigation measures,[26] and various other time-tested aspects of information security, including documentation, risk assessment, safeguard implementation, employee training, access controls, monitoring, incident response, and ongoing evaluation. This ensures that several critical areas of information security are addressed.[27] We expect these measures to bring Blackbaud up to the baseline of what all companies are expected to do to safeguard consumer data—i.e., what Blackbaud should already have been doing. We applaud the Commission for updating its orders to reflect evolving best practices, such as requiring that third-party assessments not rely primarily on assertions by management[28] and that the party consenting to the order utilize non-SMS-based MFA.[29]

EPIC urges the Commission to finalize the proposed Blackbaud consent order with the above recommendations. Please feel free to reach out to EPIC Counsel Chris Frascella at frascella@epic.org or Suzanne Bernstein bernstein@epic.org if you have any questions.

---

[23] *See, e.g.*, EPIC Commercial Surveillance Comment at 181-82; EPIC ONCD Comment at Appendix 1.
[24] Proposed Order at 7-11.
[25] *Id.* at Section IV (E)(11, 13).
[26] These include limiting password re-use, *id.* at Section IV(E)(3), terminating employee accounts when they are no longer necessary or when they are abused, *id.* at Section IV(E)(6), segmentation of systems, *id.* at Section IV(E)(9), and encryption, *id.* at Section IV(E)(12). EPIC notes that encryption is not foolproof as a means of safeguarding data, as the threat actor could also obtain the key necessary to decrypt it or encryption protocols may become obsolete as computing technology advances. *See, e.g.*, Comments of EPIC, *in re* Data Breach Reporting Requirements, WC Dkt. No. 22-21 (Feb. 22, 2023), https://epic.org/documents/in-re-data-breach-reporting-requirements/. We also note that the complaint requires traffic monitoring, timely patching, and penetration testing, which is consistent with the Commission's pattern of data security enforcement orders. *See, e.g.*, EPIC Commercial Surveillance Comment at 202-03, 207.
[27] Proposed Order at 7-11.
[28] *Id.* at Section V(D). *See also* EPIC Commercial Surveillance Comment at 208-210.
[29] *Id.* at Section IV(E)(4). *See also* Comments of EPIC, *in re* Protecting Consumers from SIM-Swap and Port-Out Fraud, WC Dkt. 21-341 (Jan. 16, 2024), https://epic.org/documents/in-re-protecting-consumers-from-sim-swap-and-port-out-fraud-fnprm/.

Respectfully submitted, this the 14th day of March 2024, by

Chris Frascella
Counsel

Suzanne Bernstein
Law Fellow

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036