Akin®

FTC's Proposed Settlement with Blackbaud Requires Data Deletion and Data Governance

February 6, 2024

Reading Time : **4 min**

By: Natasha G. Kohne, Joseph Hold

On February 1, 2024, the Federal Trade Commission (FTC) announced that it had reached a proposed settlement with that would require Blackbaud Inc. ("Blackbaud") to delete personal data it does not need to retain and upgrade its data security practices to resolve the FTC's complaint against Blackbaud stemming from a 2020 ransomware attack. Notably, per the press release from Blackbaud, the proposed settlement does not include a fine and Blackbaud neither "admitted nor denied any of the allegations made by the FTC."[1]

Specifically, Blackbaud, a technology provider that provides data services and financial, fundraising and administrative software services to companies, nonprofits, health care organizations and others, experienced a ransomware attack in 2020, where hackers used customer credentials to gain access to Blackbaud's network. According to the FTC's complaint, the hackers went undetected for three months as they created new administrator accounts and exfiltrated personal data from millions of consumers, including names, birthdates, addresses, Social Security numbers and bank account numbers. The FTC alleged that Blackbaud failed to implement "appropriate safeguards to secure and protect the vast amounts of personal data it maintains as part of the services it provides to its clients." As a result of its deficiencies, which the FTC notes include failure to segment data and delete data that is no longer needed, hackers were able to infiltrate one of Blackbaud's customer databases and then move through Blackbaud-hosted environments.

We have detailed notable requirements from the parties' proposed settlement (Order) below.

Data Deletion:

Under the terms of the Order, Blackbaud has 90 days to complete the following data governance tasks:

- Delete files containing covered information[2] not required for providing services unless the consumer requests otherwise.[3]
- Create a publicly available data retention schedule on its website establishing: (1) the purpose covered information is maintained; (2) the specific business needs for maintaining the covered information; and (3) the timeframe for deletion, precluding indefinite retention.[4]
- Provide a written statement to the FTC describing its retention schedule.[5]

Other Data Governance Requirements:

In addition to the data deletion requirements, the Order also stipulates that Blackbaud must, among other things, implement an information security program, comply with set data retention limits, have their security program assessed and provide the FTC with an annual certification.

Information Security Program. In addition to deleting data, Blackbaud must implement and maintain a written information security program within 90 days. Such program must include:

- Providing the information security program along with any updates or evaluations to the responsible senior officer and board of directors (or equivalent governing body) at least annually, and never more than 30 days after a covered incident occurs.[6]
- Designating a qualified employee or employees to coordinate the program.
- Documenting internal and external risks to the security, confidentiality or integrity of covered information at least annually.
- Designing safeguards based on the volume and sensitivity of the covered information to control for internal and external risks with features like multi-factor authentication, access control measures and encryption of sensitive information.
- Testing safeguards, including vulnerability scanning and penetration testing, at least annually and not more than 30 days after a covered incident.
- Selecting service providers capable of safeguarding covered information and contractually requiring them to implement and maintain safeguards.[7]

Data Retention Limits. Blackbaud must refrain from retaining covered information not necessary for the purposes for which it is stored, and must not misrepresent: (1) the extent of use, deletion or disclosure of covered information; (2) the extent to which privacy, security, availability, confidentiality or integrity of covered information is protected; or (3) the extent of any covered incident or unauthorized disclosure, misuse, loss, theft, alteration, destruction or other compromise of covered information.[8]

Third Party Assessment. The Order also stipulates that Blackbaud must obtain a biennial assessment of its information security program from a qualified third party, annually certify compliance of the Order through the company's Chief Information Security Officer (CISO) and report any covered incident triggering notification to a federal, state or local entity within 10 days of the notification.[9]

Annual Certification. One year after the issuance date of the Order and each year thereafter, Blackbaud must provide the FTC with a certification from its Chief Information Security Officer that: (1) Blackbaud has established, implemented and maintained the requirements of this Order; (2) Blackbaud is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the FTC; and (3) includes a brief description of all "covered incidents" during the certified period.[10]

Covered Incident Reporting. Blackbaud must report covered incidents to the FTC within 10 days of any notification to a federal, state or local entity. The report must include certain details such as the date of the incident, description of the facts, the information affected, the number of individuals affected and remediation measures taken.[11]

The terms of the Order will terminate 20 years from the date of its issuance, barring allegations of violation.

Please contact a member of Akin's cybersecurity, privacy & data protection team to learn more about this enforcement or how it may affect your company.

---

[1]Per statement made by Blackbaud, "Blackbaud Reaches Agreement with the Federal Trade Commission Related to 2020 Security Incident" https://www.blackbaud.com/newsroom/article/blackbaud-reaches-agreement-with-the-federal-trade-commission-related-to-2020-security-incident (Feb. 2, 2024)

2 The FTC specified "covered information" to include: "means information from or about an individual consumer stored by Respondent's customers within Respondent's product databases including: (a) a first and last name: (b) a home or physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) a driver's license or other government-issued identification number; (f) date of birth; or (g) bank account, credit card, or debit card information."

3 Decision and Order, *In the Matter of Blackbaud Inc.*, FTC No. 2023181 (February 1, 2024) hereinafter "Order."

4 *Id.* at 7.

5 *Id.*

6 A "covered incident" refers to "any incident that results in Respondent notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization." *Id.* at 5.

7 *Id.* at 7-10.

8 *Id.* at 6.

9 *Id.* at 11-14.

10 *Id.* at 13.

11 *Id.* at 14.

Categories

Cybersecurity, Privacy & Data Protection

Data Breach

Consumer Data Protection