Updates
February 07, 2024
FTC Brings First Standalone Section 5 Unfairness Claims for Unreasonable Data Retention and Inaccurate Breach Notice

On February 1, 2024, the Federal Trade Commission (FTC) announced a complaint and proposed consent order against Blackbaud, Inc. concerning a 2020 data security incident that included a ransomware demand and payment.

According to the FTC's complaint, Blackbaud's allegedly unfair and misleading conduct included not just deficient data security practices but also a delay in providing accurate notice to its business customers about the breach, including the inclusion of deceptive statements about the scope and severity of the breach in its initial notice to those customers. The FTC highlighted that this case is the first time it has brought standalone Section 5 unfairness claims arising out of the alleged failure to (1) implement and enforce reasonable data retention practices and (2) accurately communicate the severity and scope of the breach.

The Blackbaud Security Incident and Notice to Customers

Blackbaud provides a variety of software products and services to nonprofits, foundations, educational institutions, and healthcare organizations, including database services for tracking donors and donations. The complaint alleges that on February 7, 2020, an attacker used a customer's login to gain access to a customer's Blackbaud-hosted database. According to the complaint, the attacker was then able to leverage vulnerabilities to move across Blackbaud-hosted environments and exfiltrate files containing millions of items of consumers' personal information maintained by Blackbaud customers on the Blackbaud network. The FTC alleged the personal information included full names, birthdates, Social Security numbers, home addresses, phone numbers, email addresses, financial information (such as bank account information, estimated wealth, and identified assets), medical information (such as patient and medical record identifiers, treating physician names, health insurance information, medical visit dates, and reasons for seeking medical treatment), genders, religious beliefs, marital statuses, spouse names, spouses' donation history, employment information (including salary),

educational information, and account credentials. According to the complaint, the foregoing data was not encrypted because (1) Blackbaud allowed its customers to store Social Security numbers and bank account information in unencrypted fields not specifically designated for these purposes; (2) Blackbaud allowed customers to upload attachments containing consumers' personal information, which Blackbaud did not encrypt; and (3) Blackbaud did not encrypt its database backup files containing complete records from customers and former customers.

The complaint alleges that, after the intrusion was discovered on May 20, 2020, the attackers demanded a ransom. Although Blackbaud paid $235,000 in Bitcoin, the FTC highlighted in its complaint that Blackbaud has not been able to "conclusively verify" the stolen data was deleted. The complaint alleges that Blackbaud failed to notify its customers of the incident for two more months, until July 16, 2020, following an investigation characterized by the complaint as "exceedingly inadequate." In addition, the FTC alleges that this first notice to customers stated that no credit card information, bank account information, or Social Security numbers had been accessed and that "**[n]o action is required on your end because no personal information about your constituents was accessed.**" Although Blackbaud allegedly knew as of July 31, 2020, that bank account numbers and Social Security numbers had been exfiltrated, this fact was not disclosed to its customers until October 2020.

The FTC's Claims and Proposed Order

All five of the FTC's claims are brought under Section 5 of the FTC Act, 15 U.S.C. § 45(a), for deceptive or unfair acts or practices. Notably, the complaint brings three novel claims:

- **Unfair data retention practices.** The FTC alleges that Blackbaud engaged in an unfair practice by failing to implement and enforce reasonable data retention practices for sensitive consumer data maintained by customers in its network. According to the complaint, Blackbaud kept its customers' consumer data for years longer than necessary, contrary to its own policies—including, in some instances, the data of former customers and prospective customers.
- **Unfair, inaccurate initial breach notification.** The FTC alleges that Blackbaud's initial July 2020 notification to customers regarding the breach failed to accurately communicate the scope and severity of the breach and that this was an unfair act. The unfairness claim is predicated on both Blackbaud's allegedly inaccurate statement about the scope of the personal information that had been exposed and the months-long delay before Blackbaud provided a second, accurate notice about the scope of that data. (Blackbaud's March 2023 settlement with the SEC also concerned Blackbaud's July 2020 notification to its customers, which the SEC alleged was misleading to investors about the impact of the incident.)
- **Deceptive initial breach notification.** Relatedly, the FTC also alleges that the July 2020 initial notice containing an inaccurate statement about the extent of compromised consumer data was deceptive under Section 5.

In addition, the complaint also brings two claims familiar in FTC data security cases:

- **Unfair information security practices.** The FTC alleges that Blackbaud failed to take a variety of reasonable steps to prevent unauthorized access to sensitive personal information (e.g., allegedly deficient encryption practices and a laundry list of assertedly lax security practices, such as allowance of weak passwords, lack of multifactor authentication to protect sensitive information, deficient threat monitoring, and failure to timely patch outdated software and systems).
- **Deceptive security statements.** The FTC alleges that a statement in the Blackbaud website privacy policy that Blackbaud provided "appropriate" safeguards to protect personal information collected via the website was deceptive.

The Proposed Order

Like the complaint, the proposed order contains a mixture of provisions that are standard fare in FTC data security consent orders and others that are less common. Among the former category are provisions prohibiting Blackbaud from making misrepresentations about its privacy and data security practices, requiring it to institute a comprehensive data security program subject to third-party independent biennial assessments, and necessitating that it provide the FTC with reports on data breaches that result in Blackbaud reporting the incident to authorities under federal, state, or local law. The order also includes several additional requirements that are not unprecedented but that the FTC has included only in a subset of data security orders, depending on the alleged facts of the case:

- **Mandatory data deletion.** Requiring deletion by Blackbaud of its customer backup files that contain consumers' personal information that is not being retained in connection with providing products or services to Blackbaud's customers.
- **Data retention.** Requiring Blackbaud to make publicly available and adhere to a retention schedule for customer backup files containing consumers' personal information, to include (1) the purposes for maintaining that personal information, (2) Blackbaud's specific business needs for retaining that personal information, and (3) the set time frames for the deletion of that personal information (i.e., no indefinite retention).

Takeaways

- As the three FTC commissioners highlighted in their joint statement on the case, **this is the first time the FTC has alleged that retaining data for longer than necessary was, by itself, an unfair practice under Section 5**—although such data retention has previously been included among several data security shortcomings that allegedly rendered practices unfair under Section 5 (as in, for example, the complaint against Chegg, Inc.). By alleging this as a "standalone" unfairness claim, the FTC underscores the importance it is placing on data deletion from both a privacy and a data security standpoint.
- **This case is also the first time that the FTC has alleged that a failure to accurately communicate the scope and severity of a breach was an unfair practice**, as the commissioners also noted in their statement. This highlights that the FTC is apt to scrutinize a reassuring message about the limited scope of a data security incident, even if it is true for most affected individuals. If the message later turns out to be inaccurate as it pertains to some portion of the affected population, the FTC may see the statement as deceptive when made and reflective of a poor investigation.
- **Finally, the FTC alleges that despite paying a ransom to the attacker, Blackbaud was unable to "conclusively verify" that the exfiltrated data had been destroyed.** Given the multitude of ways that data can be copied, transferred, hidden, or recovered, it is difficult to see how remote data deletion could ever be "conclusively verified," let alone when engaging with a criminal organization operating in an unknown location—although there have not been confirmed reports that the data at issue in the Blackbaud incident has since been released or misused. Left unaddressed in the complaint is what a company in Blackbaud's situation should have done in negotiations with the attacker that would have provided any greater protection to consumers.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law

Related insights

Update

The Dismantle DEI Act: One Potential Blueprint for Forthcoming Attacks on DEI

Update

LA Fires: Employer Considerations in Light of the Disaster