ALERTS | 03.16.2023

FTC Orders BetterHelp to Pay $7.8M in AdTech Ruling

The FTC recently filed its second enforcement action related to web tracking tools (a.k.a. AdTech) and the unauthorized disclosure of health information for advertising and third parties' independent uses. The Complaint and Consent Order against BetterHelp, Inc. ("BetterHelp"), an online counseling service provider, allege that BetterHelp shared consumers' sensitive mental health information with Facebook, Snapchat, and Pinterest for targeted advertising purposes. Notably, this is the first FTC action that involves returning funds to consumers whose health data was compromised. Specifically, the $7.8 million fine will be used to provide partial refunds to consumers who signed up and paid for BetterHelp's services between August 1, 2017 and December 31, 2020. The FTC alleges that BetterHelp's conduct violates Section 5 of the FTC Act (15 U.S.C. Sec. 45(a)). BetterHelp's conduct took place prior to the FTC's issuance of its Health Breach Notification Rule (HBNR) policy statement in 2021, and so the FTC does not allege a violation of HBNR, as it did in the GoodRX enforcement action.

Background

In addition to offering general counseling services, BetterHelp provides mental health counseling to consumers through targeted client groups, including Christians, teens, those seeking marriage counseling, and the LGBTQ community. Since its inception in 2013, BetterHelp has gained over 2 million users. Today it has over 374,000 active users in the United States and 25,000 licensed therapists who provide services via video conferencing, text messaging, live chat, and audio calls.

BetterHelp's Allegedly Deceptive Privacy Practices and Misrepresentations

The FTC alleges that BetterHelp failed to provide consumers with proper notice as to the collection, use and disclosure of their personal and sensitive health information. BetterHelp made repeated assurances of privacy, including statements like: "Rest assured – your health information will stay private between you and your counselor" and "Your email address is kept strictly private. It is never shared, sold or disclosed to anyone. Even your counselor won't know your real email address." Despite these assurances, BetterHelp apparently disclosed its website visitors' and users' intake questionnaire responses (containing current health status and medical history) as well as email and IP addresses to Facebook — for the sole purpose of monetizing this highly sensitive information. The complaint further alleges that BetterHelp's Privacy Policy contained deceptive language, including the statement that sensitive information would be used only for "limited purposes," and making no mention of using or disclosing information for advertising purposes or permitting third parties to use the information for their own purposes.

The Complaint also alleges that BetterHelp neglected to safeguard the information it obtained from visitors and users by failing to train its employees properly on requirements regarding the collection, use, and disclosure of that information. Specifically, the complaint alleges that BetterHelp placed a recent college graduate with no marketing experience and little training in charge of deciding which visitor and user information was uploaded to Facebook. Additionally, BetterHelp failed to develop, implement or maintain written policies, procedures or practices related to the collection, use, and disclosure of consumers' health information to ensure that its practices complied with the representations it made to its users. Finally, BetterHelp maintained a deceptive "HIPAA" seal on its website implying that BetterHelp's privacy and information security practices were HIPAA compliant. BetterHelp removed the HIPAA seal upon receipt of a CID from the Commission in December 2020.

Key Takeaways and Lessons Learned

- Keep your company's Privacy Policy and customer-facing statements current and factually accurate. For example, a Privacy Policy should not claim "limited use" of consumer information if such information is being disclosed to third parties such as Facebook and Snapchat for advertising, as well as Facebook and Snapchat's own use. Anticipated transmissions of personally identifiable information (PII) to third parties should be disclosed in privacy policies, and businesses must obtain specific authorization for certain disclosures or risk financial and administrative penalties.
- Review contracts with third parties to ensure they contain language appropriately limiting how the third party can use consumer health information (as opposed to giving blanket approval for such companies to use the information for their own research and product development).
- Ensure staff is appropriately trained on policies, procedures and practices with respect to the collection, use and disclosure of user health information – and ensure that compliance with internal policies is monitored.
- Do not put a HIPAA seal on your company's website or otherwise imply that your company is "HIPAA compliant." No regulatory agency or certification entity has been authorized to conduct assessments of HIPAA compliance, and therefore no entity has the ability to claim that it has received a "HIPAA compliance" seal of approval.
- Companies must obtain express authorization before collecting, using and disclosing consumers' health information for marketing purposes.

Printable version.

Adam J. Bookbinder
Co-Chair, Government Enforcement & Compliance

Christine G. Savage
Co-Chair, Government Enforcement & Compliance