Arnold & Porter

February 15, 2023

FTC Fines GoodRx $1.5 Million in First Enforcement Action Brought Under Health Breach Notification Rule

Enforcement Edge: Shining Light on Government Enforcement

By Nancy L. Perkins, Jason T. Raylesberg, Jami Vibbert, Alex Altman

On February 1, 2023, approximately two years after the Federal Trade Commission (FTC) warned developers of health apps and connected devices, as well as other companies dealing with identifiable health information, that they may have notification obligations regarding personal health record (PHR) identifiable health information they maintain under the agency's Health Breach Notification Rule(HBNR, 16 C.F.R. Part 318), the FTC announced a proposed settlement in its first-ever enforcement action under the rule. The FTC alleged that digital health platform GoodRx violated the HBNR by failing to notify the FTC that it had shared the PHR identifiable health information of millions of users with third-party advertisers and others without the users' authorization. Under the proposed stipulated order, GoodRx, which offers prescription drug discounts and telehealth visits, will be required to pay a $1.5 million civil penalty and will be prohibited from sharing users' PHR identifiable health information with third parties for most advertising purposes. The proposed settlement illustrates the FTC's willingness to scrutinize widespread industry practices involving consumers' health information outside of the data breach context and is the latest demonstration of federal agencies' increasingly aggressive regulation of health data and online tracking technologies contained in health-related websites andapps.

In its complaint, the FTC alleged that GoodRx promised its users in a privacy policy that it would share their personal data, including health information, only with limited third parties and only for limited purposes. The privacy policy also allegedly provided that GoodRx would never share users' health information with advertisers. GoodRx, the FTC claimed, repeatedly breached these representations by disclosing PHR identifiable health information to advertisers such as Facebook and other third parties. According to the FTC, more than 55 million consumers have visited or used GoodRx's websites or mobile apps since January 2017. While the HBNR initially may have been understood as a means to address data breaches (defined as "unauthorized" acquisitions of PHR identifiable health information), according to the FTC, GoodRx's failure to notify the Commission and other parties about the intentional, company-authorized sharing of PHR identifiable health information violated the HBNR.

In addition to the HBNR violation, the FTC also asserted seven causes of action under Section 5 of the FTC Act (Section 5), which prohibits unfair and deceptive practices harmful to consumers. The Section 5 claims contain allegations that GoodRx made misrepresentations regarding (1) its disclosures of personal and health information to third parties; (2) third-party uses of health information it shared; and (3) its compliance with the Digital Advertising Alliance Principles and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The FTC further alleged that the health platform did not implement measures to safeguard against the unauthorized disclosure of health information and failed to provide notice and obtain consent before using and disclosing such information for advertising purposes. The FTC deemed the last two allegations "unfair" practices under Section 5. While the FTC has often focused its privacy violation inquiries on whether data collection and disclosure practices were "deceptive" in nature, the Commission appears to be ramping up privacy unfairness claims by taking action such as suing a digital marketing and analytics company for the "unfair sale of sensitive data." The proposed GoodRx settlement suggests the FTC intends to continue building on this precedent to enforce substantive, and not just procedural, restrictions on how businesses collect and disclose health information. It also suggests that the Commission plans to use enforcement authority with fining power (including under the HBNR and the Children's Online Privacy Protection Rule) to add weight to its Section 5 privacy allegations.

The proposed settlement will require GoodRx to implement a comprehensive privacy program with strong data protection safeguards. Samuel Levine, director of the FTC's Bureau of Consumer Protection, stated: "Digital health companies and mobile apps should not cash in on consumers' extremely sensitive and personally identifiable health information. The FTC is serving notice that it will use all of its legal authority to protect American consumers' sensitive data from misuse and illegal exploitation." Businesses, particularly those simultaneously managing health information (even consumer health information) and advertising, should consider this enforcement action as a reminder to continually review and update their privacy notices and policies to accurately reflect their data collection and

disclosure activities. They should review and refine internal policies and procedures to align with privacy laws and regulations. Moreover, the proposed settlement should prompt companies to consider how they evaluate third parties with whom they share health information, including by conducting thorough diligence in the partner/vendor selection process and imposing appropriate contractual obligations on business partners and vendors who receive health information.

** Tamuz Avivi contributed to this blog post. Ms. Avivi is a graduate of Columbia University School of Law and is employed at Arnold & Porter's New York, NY office. Ms. Avivi is not admitted to the practice of law in New York.*