

JULY 30, 2026 | PUBLICATION

Client Alert: FTC and States Sue Hims & Hers Over Deceptive Health Data Sharing and Subscription Billing Practices

Executive Summary

On July 29, 2026, the Federal Trade Commission (FTC), joined by co-plaintiffs the State of Utah and the County of Los Angeles (acting through the Los Angeles County Counsel on behalf of the People of the State of California), filed a federal complaint in the Northern District of California against Hims & Hers Health, Inc. (*FTC et al. v. Hims & Hers Health, Inc.*). The complaint alleges that the major telehealth provider shared consumers' sensitive health information with third-party advertising platforms, including Meta and Snap, despite marketing its services as private and discreet, and that it engaged in deceptive and unlawful subscription billing and cancellation practices. The enforcement action invokes Section 5 of the FTC Act and the Restore Online Shoppers' Confidence Act (ROSCA). This alert summarizes the key allegations, legal theories, and practical takeaways for companies operating in digital health, telehealth, and consumer-facing subscription industries.

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Background: Hims & Hers and the Telehealth Landscape

Hims & Hers Health, Inc., headquartered in San Francisco, is one of the largest direct-to-consumer telehealth platforms in the United States. Founded in 2017, the company offers telehealth appointments and prescription medications, shipped directly to consumers, for conditions including weight loss, erectile dysfunction, hair loss, and mental health. The company is a significant player in the growing market for GLP-1 weight-loss medications and has relied heavily on celebrity brand ambassadors (including Kristen Bell, Rob Gronkowski, Miley Cyrus, and Alex Rodriguez) and paid social media influencers, many of whom described the platform's services as "discreet," reinforcing privacy-centric marketing claims.

The FTC's action is part of a broader regulatory trend targeting digital health companies' use of consumer health data for advertising purposes, an area that has drawn heightened scrutiny from federal and state regulators.

Summary of Allegations

A. Unauthorized Sharing of Sensitive Health Information

The complaint alleges that Hims & Hers shared consumers' sensitive health information with third-party advertising platforms, including Meta and Snap, notwithstanding the company's representations that it would protect patient privacy. According to the FTC, this sharing occurred through two primary mechanisms:

- **Customer Lists:** Hims allegedly shared lists of certain customers, identified by their health conditions or treatment types, directly with advertising platforms for targeted ad campaigns.
- **Website Tracking Technologies (Events):** Third-party tracking pixels and Software Development Kits (SDKs) embedded on Hims' website automatically transmitted certain user actions (Events) to advertising companies, disclosing information about consumers' interactions with health-related content and services.

These practices allegedly occurred despite Hims' privacy representations to consumers, including marketing by influencers emphasizing the "discreet" nature of the service.

B. Deceptive Billing and Charging Practices

The complaint further alleges that Hims failed to clearly disclose that it charges consumers for prescriptions almost immediately after they submit an intake form, notwithstanding representations that consumers would be able to consult with a medical provider to find a treatment "right for them." According to the FTC, most customers did not receive a consultation with a provider before being charged.

C. Difficult Cancellation Process and Early Refill Charges

The FTC alleges that Hims advertised monthly or quarterly refill schedules but processed refill charges approximately 10 days earlier than consumers would reasonably expect and required cancellation two days before that early processing date—making it easy for consumers to miss the deadline. The complaint also alleges that Hims made it unreasonably difficult for consumers to cancel their subscriptions.

Legal Theories

The enforcement action relies on two primary statutory bases:

- **Section 5 of the FTC Act (15 U.S.C. § 45):** The complaint alleges both deceptive practices

(misrepresentations regarding privacy and billing) and unfair practices (sharing sensitive health data without adequate consumer consent and charging consumers before providing promised consultations).

- **Restore Online Shoppers' Confidence Act (ROSCA) (15 U.S.C. §§ 8401–8405):** ROSCA prohibits charging consumers for goods or services through a “negative option” feature unless the seller clearly and conspicuously discloses the material terms of the transaction, obtains the consumer’s informed consent, and provides a simple mechanism for cancellation. The FTC alleges that Hims’ subscription practices violated each of these requirements.

State Co-Enforcement: California and Utah

Notably, the FTC was joined by the State of Utah and the County of Los Angeles (acting on behalf of the People of the State of California). The involvement of state and local co-plaintiffs reflects a growing trend toward coordinated federal-state enforcement in data privacy and consumer protection matters. This joint approach signals that:

- State attorneys general and local counsel offices are increasingly active partners in federal data privacy enforcement, particularly in the digital health space.
- Companies operating in telehealth and digital health should expect scrutiny not only from the FTC but also from state regulators applying parallel state consumer protection and privacy laws.
- Coordinated enforcement can expand the scope of potential remedies and may increase settlement leverage.

Practical Takeaways and Action Items

Companies in digital health, telehealth, and other consumer-facing industries should consider the following in light of this enforcement action:

Health Data Sharing with Advertising Platforms

- Audit all third-party tracking technologies (pixels, SDKs, cookies, server-side integrations) deployed on websites and mobile applications, with particular attention to pages or flows involving health information.
- Evaluate whether customer lists shared with advertising platforms for audience targeting could be construed as disclosing health information (e.g., lists segmented by medical condition or treatment type).
- Review privacy policies and consumer-facing disclosures to ensure they accurately describe data sharing practices with advertising technology partners. Avoid broad privacy promises that are inconsistent with operational practices.
- Consider whether health-related “Events” transmitted by website tracking technologies constitute sharing of sensitive health information under applicable federal and state law.

Privacy Representations and Marketing

- Ensure that marketing claims, including those made by brand ambassadors, influencers, and affiliates, are consistent with actual data practices. Representations of “discretion” or “privacy” may be treated as affirmative claims that create enforceable obligations.
- Implement compliance review processes for influencer and third-party marketing content to ensure consistency with privacy practices.

Subscription Billing and Cancellation (ROSCA and State Laws)

- Review subscription enrollment flows to confirm that all material terms, including when charges will be processed relative to service delivery, are clearly and conspicuously disclosed before the consumer is charged.
- Ensure that cancellation mechanisms are simple and accessible. Note that the FTC's "Click-to-Cancel" rule (effective 2024–2025) and analogous state laws (e.g., California's automatic renewal laws) impose specific requirements on the ease of cancellation relative to the ease of enrollment.
- Evaluate refill and renewal timing practices to confirm they align with consumers' reasonable expectations based on the company's marketing and disclosures.
- Do not charge consumers for products or services before delivering on the promised value (e.g., a provider consultation) that was a material inducement to purchase.

Broader Compliance Considerations

- This action is part of a broader FTC enforcement trend targeting digital health companies' data practices. Companies in this sector should proactively assess compliance with FTC guidance on health data, including the Health Breach Notification Rule and prior enforcement actions.
- Companies should anticipate multi-jurisdictional scrutiny and ensure compliance not only with federal requirements but also with state consumer protection statutes and emerging state health data privacy laws.

Status of the Matter

This is a developing matter. A complaint has been filed; the allegations have not been proven, and no court has made any findings of liability. We will continue to monitor this case and provide updates as it progresses.