Insights, News & Events

HEALTHLINE TO PAY $1.55M FOR ALLEGED CCPA VIOLATIONS: KEY LESSONS FOR BUSINESSES FROM LARGEST SETTLEMENT YET

Insights
Jul 7, 2025

Healthline Media has agreed to pay $1.55 million to resolve allegations that it violated the California Consumer Privacy Act (CCPA) – which is the largest settlement to date under the state's landmark privacy law. The California Attorney General alleged that the company's health information website, Healthline.com, failed to allow consumers to opt out of targeted advertising and shared data – including information about potential medical conditions – with third parties without proper privacy protections. The settlement, which still needs to be approved by the court, also contains a unique provision: it prohibits Healthline from sharing information with third parties about article titles consumers view that may reveal a medical diagnosis. Here's a breakdown of the allegations and settlement terms, as well as a six-step compliance plan for businesses that operate in California or collect data from California residents.

Background and Allegations

Healthline.com is one of the top 40 most visited websites in the world, according to the California Attorney General's July 1 settlement announcement. The website provides health and wellness information to consumers and gets paid through third-party ads, which may personally target readers. Here are the key facts and allegations according to the state:

- Healthline allowed online trackers, like cookies and pixels, to share data about readers with third parties, including information that could be used by the third parties to identify the consumer.

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627

Usama Kahf, CIPP/US

Partner

949.798.2118

- Third parties could also see the article titles that consumers were reading, which may reveal a medical diagnosis. For example, an article may be titled: "You've Been Newly Diagnosed with MS. What's Next?"
- Dozens of trackers were sharing consumer data with numerous third parties.
- Healthline allegedly violated the CCPA and the state's Unfair Competition Law by:
  - Failing to allow consumers to **opt out of sharing their personal information** for targeted advertising. The complaint said Healthline shared data with advertisers even after consumers opted out.
  - Violating the "**purpose limitation principle**," which limits a business's use of personal information to the purposes for which it was collected or processed – or another disclosed, compatible purpose. Healthline is accused of sharing article titles that might reveal a consumer's medical diagnosis.
  - Failing to maintain **CCPA-required contracts**. Advertising contracts should contain certain data privacy protections that are required by the CCPA. The Attorney General alleged that Healthline assumed but did not verify that third parties agreed to follow the appropriate framework.
  - Misleading consumers about privacy practices in violation of the Unfair Competition Law rules against **deceptive business practices**. Healthline.com allegedly featured a "consent banner" that claimed to – but did not – disable tracking cookies when consumers unchecked a box.

Notably, Healthline is also facing a class action in federal court and a separate individual claim in state court under the California Invasion of Privacy Act (CIPA) for use of tracking technology on its website.

The Settlement

Under the proposed settlement with the California Attorney General, Healthline has agreed to:

- Pay $1.55 million in civil penalties;

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

- Ensure its opt-out mechanisms work correctly;
- Refrain from disclosing information that can link a specific consumer to an article title indicating a medical diagnosis;
- Maintain a CCPA compliance program that includes contract audits that ensure required privacy terms are included or confirm that third parties have signed an industry contractual framework that includes the appropriate terms; and
- Maintain accurate online disclosures and a privacy policy.

Lessons for Businesses: Your 6-Step Compliance Plan

The Healthline lawsuit and settlement demonstrate California officials' commitment to enforcing the CCPA and highlight the importance of creating a robust compliance plan. For any business that operates in California or collects data from California residents, here are six key steps you should consider taking to reduce privacy risks:

1. Know What Cookies Are on Your Site: A frequent issue businesses face is that they are unaware of what technology is on their websites. This can be for myriad reasons. For example:

- the website has had multiple external vendors responsible for its maintenance;
- there has been internal turnover of employees responsible for website maintenance;
- multiple individuals or departments have the ability to change what technologies are on the website; or
- the website has been active for years and there is no program in place to record or manage onboarding and offboarding of tracking technologies.

Businesses cannot fix what they do not know is there – and many times discover that their website has tracking technologies that nobody is using and serve no business purpose. In such cases, a fast path towards compliance can be to identify and remove tracking technology that serves no purpose.

2. Understand What Your Cookies Collect and Disclose: A frequent issue is that businesses may not realize what

information is being disclosed to third parties through cookies and other tracking technology on their websites. If you have any tracking technology on your website, it is critical to have ongoing technical testing as data leakages can occur if the settings are even slightly off. Consider having such technical-testing vendors be retained through legal counsel to ensure the protection of the attorney-client privilege and attorney work product.

3. Consider What Disclosure is Within the Reasonable Expectation of the Consumer: The AG emphasized that the disclosure of personal information to third parties may be unlawful – even if the fact this is happening was disclosed in a privacy policy where the disclosure differs "substantially" from the consumer's reasonable expectations. This is going to be a context-specific analysis and will also consider the nature of the personal information and the nature of your business. If you need a quick rule of thumb, be wary of disclosing, "selling," or "sharing" sensitive personal information (as defined by the CCPA or other relevant state consumer privacy laws applicable to your business) for purposes of targeted advertising.

4. Be Sure Opt-Out Mechanisms are Functional: Regularly test your cookie banner and consent process to make sure it actually works, and do not simply rely on the provider of such software to ensure it continues to do what it's supposed to do. It is ultimately your responsibility to ensure that all cookies are properly classified and that opt-outs and opt-ins to cookies work as intended.

5. Ensure Vendor and Third-Party Contracts are CCPA-Compliant: Businesses are responsible for ensuring contracts with service providers, contractors, and third parties comply with CCPA requirements and include provisions aligned with their job functions. Third parties include vendors who "sell" or "share" personal information, such as advertising vendors – although the contract terms for such third parties will be different than the contract terms for your services providers and contractors. If you have not checked that all your website vendors have appropriate contractual terms, now is the time to do so.

6. Seek Guidance on Data Privacy Compliance: If your business is unsure where it stands on privacy compliance, now is the time to act. A proactive review of privacy practices could help you avoid costly penalties and strengthen your customer relationships in the process. Our

team regularly advises companies on CCPA/CPRA, GDPR, and global privacy frameworks. Contact us to schedule a consultation or privacy assessment.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group or Consumer Privacy Team.