Insights, News & Events

CLOTHING RETAILER FACES BIG FINES FOR CCPA VIOLATIONS: A WAKE-UP CALL + AN ACTION PLAN FOR BUSINESSES

Insights
May 15, 2025

In a significant enforcement move, California's consumer privacy regulator just ordered a national clothing retailer to pay a $345,178 fine to resolve alleged violations of the state's privacy law. The California Privacy Protection Agency (CPPA) said in its order that Todd Snyder, Inc. collected and processed the personal information of California consumers who interacted with its website between November 1, 2023 and December 31, 2024. In addition to the financial penalty, the retailer must implement corrective measures to align its data-handling practices with the California Consumer Privacy Act (CCPA). This enforcement action sends a clear message: data privacy compliance is no longer optional, especially for consumer-facing brands collecting personal information online. Here's what you need to know about the order and what it means for your business.

Key Allegations Against the Retailer

The Todd Snyder case shows that penalties can be imposed purely for procedural and structural non-compliance under the CCPA, even if no breach or misuse occurs. The CCPA's May 1 order makes the following notable allegations:

- **Inequitable Consent Mechanisms:** For 40 days starting in late 2023, the website's opt-out mechanism (which should enable consumers to exercise their choices) was not properly configured. It was also impossible for consumers to submit their request to opt-out from the company selling and sharing their personal information.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118

Xuan Zhou, CIPP/US, CIPM, CIPP/E
Associate
858.597.9632

- **Unlawful Verification Standard to Request Opt-Out:** The company required consumers to provide their first name, last name, email, country of residence, and a selfie photo to submit their request to opt-out of sale/sharing, which is a violation of California law.
- **Excessive Data Collection:** The company was accused of unlawfully requiring consumers to submit more information than necessary to opt out, including government identification to verify that the specific consumer or an authorized person is making the request.

A 6-Step Action Plan for Businesses

The enforcement action underscores the CPPA's commitment to holding businesses accountable for non-compliance with the state's landmark privacy law. 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. **Avoid Collecting Unnecessary Data During Privacy Requests:** Review and update your data collection practices ensuring that only necessary personal information is collected from consumers.
2. **Offer Real Choice Through Consent Mechanisms:** Businesses should provide equal and clear options for consumers to easily manage their privacy preferences.
3. **Be Sure Opt-Out Mechanisms are Clear, Functional, and Fair:** Businesses should not only provide a "Do Not Sell or Share My Personal Information" link, but also ensure that the opt-out process is intuitive, equitable, and does not require consumers to provide unnecessary personal information to exercise their rights. 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.
4. **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.

Service Focus

Consumer Privacy Team

Privacy and Cyber

Industry Focus

Retail

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

5. **Maintain An Up-to-Date Privacy Policy:** Ensure your business privacy policy clearly outlines what personal data is collected, how it's used, the rights consumers have under the CCPA, and how they can contact your business with privacy-related questions or requests.

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 direct 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 author of this Insight, or any member of our Privacy and Cyber team.