VENABLE LLP

Retailer Todd Snyder Fined for CCPA Violations Related to Opt-Out Compliance, Vendor Management, and Data Collection

May 15, 2025

Michael A. Signorelli, Rob Hartwell and Chelsea Reckell Richmond

Another month brings another California Privacy Protection Agency (CPPA) enforcement action, the agency's second enforcement action under the California Consumer Privacy Act (CCPA).

The May 1st order against fashion retailer Todd Snyder, Inc. imposes a fine of $345,178 and mandates comprehensive reforms to the company's privacy practices, following a series of alleged violations affecting consumer opt-out rights and data request handling. This action further emphasizes the CPPA focus on verification, cookie banners and vendor oversight, and data minimization.

CCPA Enforcement Highlights: Lessons from the Todd Snyder Fine

Technical Glitches Aren't an Excuse

The CPPA found that Todd Snyder failed to honor consumer opt-out requests for 40 days because of a misconfigured cookie consent banner. Consumers were told they could manage their preferences through a "Cookie Preferences Center," but when they clicked the link, a cookie consent banner appeared briefly and either disappeared or failed to work properly. The CPPA alleged this configuration prevented users from submitting opt-out of sale and sharing requests. The same configuration issue blocked recognition of Global Privacy Control (GPC) signals.

The CPPA emphasized that businesses cannot shift responsibility to third-party vendors without confirming the tools' functionality. In Todd Snyder's case, the agency found that the company "deferred to third-party privacy management tools without knowing their limitations or validating their operation." Companies should test and validate their consent management systems regularly to ensure that opt-out signals—including GPC—are properly received and acted upon by the company and its vendors. This action follows on an earlier focus on cookie banners by the CPPA and other regulators.

Improper Verification of Opt-Out Requests Is a Violation

The CPPA also alleged that Todd Snyder imposed an unlawful verification requirement on consumers

attempting to opt out of personal data sales or sharing. The CCPA exempts opt-out requests from verification requirements. However, Todd Snyder's privacy portal required a government-issued ID for all requests, including those to opt out of sale/sharing.

The CPPA found that this practice exceeded what the law permits, discouraging consumers from exercising their rights—contrary to the CCPA's goal of minimizing friction in asserting privacy choices. The CPPA's discussion serves as a warning that request procedures must be tailored to the CCPA's specific requirements for each consumer right and that opt-outs should not be subject to verification requirements.

Limit Data Used for Verification to What's Legally Necessary

Beyond applying a blanket verification standard, the CPPA also alleged that the company collected more information than was necessary to process consumer requests. This included requests for government-issued IDs for verification of verifiable requests instead of matching against data already maintained by the business. The CPPA characterized this as "discouraging consumers from submitting CCPA requests" and noted that it violated CCPA limits on collecting sensitive personal data unless necessary.

In light of this action, companies should assess ID verification procedures to confirm compliance with CCPA requirements.

Required Contract Management Reforms

As part of the final order, Todd Snyder agreed to implement a wide range of corrective actions, which notably includes implementing a contract management and tracking process to ensure all terms required by the CCPA are in place with recipients of personal data. The inclusion of this requirement suggests that the CPPA continues to emphasize the adequacy of contractual safeguards for personal data.

What Businesses Should Do to Stay CCPA Compliant

Businesses should review third-party tools for CCPA implementation, audit their opt-out mechanisms and tracking disclosures on a regular basis, and carefully review implementation of verification standards. Companies should also ensure their vendor agreements are up to date and tracked for easy review.

If you would like help determining how to use these types of tools effectively, contact the authors or visit Venable's Privacy and Data Security web page.