

# Publications

October 2, 2025 • Updates

## \$1.35M CPPA Fine Signals New Focus on Privacy Disclosures

### Key Takeaways

- The CPPA fined Tractor Supply \$1.35 million — more than double its previous largest penalty — for failing to comply with privacy notice and consumer rights requirements.
- This is the agency's first enforcement action targeting job applicant notices and failure to update privacy disclosures annually.
- Businesses should expect heightened scrutiny and broader enforcement, including multi-year compliance obligations for violators.

Earlier this week, the California Privacy Protection Agency (CPPA) levied the agency's largest fine under the California Consumer Privacy Act. Announced on Sept. 26, the \$1.35 million fine is the third enforcement action brought by the agency and a steep jump compared to its prior penalties — double the \$632,500 amount levied against Honda in March 2025 and four times the CPPA's second enforcement action against Todd Snyder for \$345,000. The record-breaking settlement signals the CPPA's continued push for meaningful compliance with the state's comprehensive data privacy law.

### CPPA Expands Focus Beyond Data Rights

To date, the CPPA has primarily focused on enforcing data subject rights. While that remains a key issue here, this settlement marks the first time the agency has addressed noncompliance with other aspects of the law — notably, the Act's requirements to provide proper privacy notices to consumers and job applicants.

Under the Act, covered businesses are required to provide a privacy notice to consumers (including job applicants) that:

1. addresses how the business processes consumer personal information; and
2. informs consumers about the rights they have and how to enforce those rights.

According to the settlement, Tractor Supply failed on multiple fronts. It did not disclose the categories of personal information it collected or shared; address the specific rights that California consumers have regarding their personal information; or explain how consumers could exercise their rights.

### Related People

- Pavel (Pasha) A. Sternberg
- Aaron A. Ogunro

### Related Capabilities

- Privacy & Cybersecurity
- US State Privacy Laws

## Job Applicant Notices Now Under the Microscope

Unique among state privacy laws, the CCPA is the only comprehensive state privacy law that also applies to job applicants. According to the settlement, while Tractor Supply maintained a California-specific notice for job applicants, it failed to include any information about their rights or how job applicants could exercise them under the CCPA.

Separately, the CPPA made clear that businesses are required to update their privacy notices **annually**. Tractor Supply failed here as well — it had not updated its privacy notice in four years.

Consistent with the CPPA's other enforcement actions, Tractor Supply was also penalized for:

1. failing to have adequate contractual provisions with vendors to limit downstream entities from processing and using personal information; and
2. failing to adequately offer and honor consumer opt out requests for the sale/sharing of personal information. Tractor Supply's webform did not opt consumers out of the sale or sharing of their personal information, and it failed to honor opt-out preference signals.

## Remedial Measures Go Beyond the Fine

As with all enforcement actions by the CPPA, the financial penalty is just one piece of the imposed penalty. Tractor Supply must also implement other remedial measures, including having a corporate officer or director annually certify Tractor Supply's compliance with the CPPA for the next four years.

## What Businesses Should Do Now

The takeaway is clear: the CPPA is actively enforcing its authority under the Act. Covered businesses should ensure compliance by:

- reviewing its privacy notices at least annually;
- correctly calibrating its website trackers; and
- building adequate processes by which to effectuate consumer rights requests.

Polsinelli's privacy compliance team has significant experience with navigating the constantly evolving data privacy law landscape. Please reach out to our team for further guidance.