

CALIFORNIA BREAKS NEW GROUND WITH RECORD \$1.35M FINE FOR JOB APPLICANT MISTAKES: 6-STEP ACTION PLAN FOR EMPLOYERS

Insights
Sep 30, 2025

The California Privacy Protection Agency, the state's main data privacy regulator, just announced its largest fine yet – a record-setting \$1.35 million – against an employer that it found to have violated job applicant and consumer privacy rights. Today's announcement marks the first-ever enforcement action involving job applicants, kicking off a new chapter when it comes to the way employers need to think about the California Consumer Privacy Act (CCPA). If you collect information from California job applicants, employees, or consumers, you will want to review our summary of this groundbreaking news and follow our six-step action plan.

What Happened?

The California Privacy Protection Agency (CPPA) launched its investigation against Tractor Supply, the nation's largest rural lifestyle retailer, after it received a solitary complaint from a consumer in Placerville, CA. It is not publicly known whether this consumer was a job applicant, employee, website user, retail customer, or other consumer. But the reality is that a CPPA investigation can be triggered by any complaint, including from disgruntled former employees or from a current employee seeking to shield themselves from retaliation, or from a job applicant who was turned away or not considered for the job.

[According to the September 30 agreement](#), the agency found that the employer failed to:

- Provide a **compliant privacy notice** to job applicants

Related People



Kate Dedenbach, CIPP/US
Of Counsel

[248.901.0301](tel:248.901.0301)



Usama Kahf, CIPP/US
Partner

[949.798.2118](tel:949.798.2118)

- Inform **job applicants of their rights** and how to exercise them
- Maintain a legally sufficient **privacy policy**
- Honor **opt-out requests** submitted through its website
- Recognize browser-based **opt-out preference signals** (like Global Privacy Control) that consumers can use to automatically indicate that they don't want their data sold or shared for targeted advertising purposes
- Enter into appropriate contracts that limit how **third-party vendors** could use shared personal data and ensure they recognize opt-out signals
- Use proper contracts with **advertising and analytics providers**

5 Reasons Why This Development is Big News for Employers

There are at least five unique factors at play here that make today's announcement a particularly significant development for employers.

1. *Applicant and Employee Data is Fully Covered*

California is so far the only state that subjects employee data – including job applicant data – to comprehensive privacy obligations. This is the first CCPA enforcement decision to make that explicit. If you have employees in the state of California or receive job applications from California residents (even if for jobs that ultimately will be outside California), this fine should serve as a wake-up call. And while this enforcement against was taken against a retailer that interacts directly with individual consumers, even businesses that are entirely B-2-B (meaning they only do business with entities, not with individuals) are at risk of being targeted for CCPA violations related to job applicant and employee privacy rights.

2. *Largest Fine Ever From CPPA*

While the state [Attorney General levied a \\$1.55 million penalty for CCPA violations earlier this year](#), today's announcement marks the largest-ever fine issued by the state's privacy agency.



**Kile E. Marks, FIP,
CIPP/US, CIPM, CIPT**

Associate

858.964.1582

Service Focus

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

3. Any Industry is Fair Game

Today's fine was against a retail company, not a tech platform, data broker, or other cutting-edge business model. "We will continue to look broadly across industries to identify violations of California's privacy law," [said Michael Macko](#), the agency's enforcement chief. In other words, the agency wants everyone to know that privacy enforcement will reach any and all sectors. If you do business in California, you're on notice.

4. Investigations Can Get Big Quick

The agency opened this case after a single individual complained. It bloomed from that one complaint to the state agency's largest-ever settlement. That means call centers, online forms, job portals, and recruiting platforms are especially vulnerable to these kinds of enforcement actions.

5. Self-Correction Doesn't Erase Liability

It seems that the right to cure isn't a cure all. The company agreed to correct many of the issues once the agency began its investigation in 2024, but its clean-up actions were too little, too late for the agency. In other words, you can't bank on cleaning up your mess after the agency has identified it as a problem. You will want to take proactive steps to get your house in order *before* your organization is targeted.

6-Step Action Plan for Employers and Businesses

Here are the six most immediate compliance steps you can take to stay ahead of the curve and minimize your chances of being the next organization to face a CCPA investigation.

1. Update Your Privacy Notices for Applicants and Employees

Make sure you provide a CCPA notice for job applicants and workers that clearly discloses rights (access, deletion, correction, opt-out, etc.). It should also include the methods that applicants and employees can use for submitting requests related to their data, which is almost always more complex and plentiful than the data collected from regular website visitors and other consumers. We recommend posting a job applicant privacy notice on your website combined with a job applicant privacy policy, all separate from your website privacy policy. You should also adopt and annually update an employee privacy policy that is separate

from your employee handbook, and make the policy available and accessible to all current and former employees.

2. Audit Job Portals, Application Systems, and Employee Platforms

It's not enough to set up systems, you need to check that they are working as intended. You should verify opt-out methods to make sure they actually work. Confirm that your website cookie consent management system detects and respects consumers' preference signals (e.g., GPC). To the extent that any of your forms or notices contain misleading language, you should edit them to remove or correct the information and avoid "dark patterns," another agency enforcement priority.

3. Review Vendor and AdTech Contracts

Today's settlement demonstrates yet again that third parties can get you in trouble. Ensure that your vendor agreements define the specific purpose that data will be used for. Your agreements should restrict third parties from secondary use, retention, or sharing of the data they have access to. To the extent you have older or generic contracts in place, you will want to update and re-negotiate them immediately.

4. Scan for Tracking Technologies

Catalog all the website cookies, pixels, scripts, trackers, and analytics tools you have in place, and confirm that your contracts and settings support user rights to the maximum extent possible. You should also assign responsibility for ongoing monitoring to a responsible party within your organization.

5. Establish a Data-Sharing Inventory

Track which platforms receive personal data, and record which rights apply and how they handle opt-outs. Plan for annual or quarterly reviews of these platforms to make sure you remain in compliance.

6. Train HR, Marketing, and IT Teams

All of these steps will be worthless if your team is not monitoring and enforcing them. Reinforce your obligations for applicant data and cover privacy request workflows with

your HR, Legal/Privacy, and IT teams. Clarify with your team the responsibilities they have when using third parties.

What's Next?

Under the settlement, Tractor Supply must – for the next five years – conduct tracking technology audits of its own website (quarterly), monitor opt-out compliance, retrain staff, and publicly report privacy metrics on its website (annually). It will also have to conduct an annual audit of the actions taken by third parties with which it shares data. That's a preview of what your organization may face if you fall behind.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as needed, 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](#).