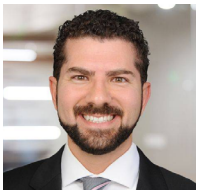
California Breaks New Ground With Record $1.35M Fine for Job Applicant Mistakes: 6-Step Action Plan for Employers

A Practical Guidance® Article by Kate Dedenbach, CIPP/US, Usama Kahf, CIPP/US, and Kile E. Marks, FIP, CIPP/US, CIPM, CIPT, Fisher & Phillips LLP

Kate Dedenbach, CIPP/US
Fisher & Phillips LLP



Usama Kahf, CIPP/US
Fisher & Phillips LLP

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Fisher & Phillips LLP

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
- 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.

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 CPPA 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.

Related Content

Resource Kit

- California Consumer Privacy Resource Kit (CCPA and CPRA)
- Employee Privacy Resource Kit
- Vendor and Service Provider Risk Management Resource Kit
- Screening and Hiring Resource Kit

Practice Notes

- California Consumer Privacy Compliance (CCPA and CPRA)
- Screening and Hiring (CA)
- California Privacy Rights Act (CPRA): Employer Obligations
- Privacy Compliance Program Management: Key Considerations and Best Practices
- Privacy Notice and Policy Drafting (CCPA/CPRA)
- Privacy Notice Requirements (CA)
- Consumer Data Privacy (CA)
- California Consumer Privacy Compliance (CCPA and CPRA)
- Third-Party Vendor Data Privacy Risk Management
- Personal Data Processing Agreement Requirements

Templates

- Privacy Notice at Collection (CCPA/CPRA) for California Employees
- Privacy Notice at Collection (CCPA/CPRA) for California Independent Contractors
- Privacy Policy (CCPA/CPRA)
- Data Processing Agreement

Kate Dedenbach, CIPP/US, Of Counsel, Fisher & Phillips LLP

Kate Dedenbach, Of Counsel in Fisher Phillips' Birmingham Michigan Office, is a data privacy attorney and Co-Chair of the Financial Services Industry Group. With 16 years of experience in data privacy, she helps businesses navigate the complex landscape of global data privacy laws, including GLBA, HIPAA, GDPR, CCPA and other state consumer privacy laws, TCPA, CAN-SPAM, and emerging AI regulations.

As a former Global Chief Privacy Officer for a large multinational financial services company, Kate offers a unique perspective. She understands how to integrate compliance with business growth, collaborating with teams in technology, product development, and marketing to build privacy-forward solutions.

A CIPP/US-certified professional, Kate's expertise includes:

- Identifying and mitigating data privacy and security risks, including conducting comprehensive data privacy reviews to identify and remediate gaps, develop data management programs, and establish internal policies and procedures for compliance with applicable laws.
- Advising employers on employee monitoring laws and implementing policies.
- Advising on compliance with state, federal, and international privacy laws, including the CCPA, GDPR, PIPEDA, and similar laws throughout the U.S. and in other countries.
- Guiding companies on website privacy mitigation steps.
- Intra-company data sharing compliance under GLBA.
- Advising companies on compliance with FCRA and state and local background screening laws.
- Review of vendor agreements and drafting and negotiation of data protection agreements with third-parties.
- Drafting and implementing policies for data sharing and AI.

Usama Kahf, CIPP/US, Partner, Fisher & Phillips LLP

Usama Kahf, a partner in Fisher Phillips' Irvine office and a Certified Information Privacy Professional (CIPP/US), co-chairs the firm's AI, Data, and Analytics Practice Group as well as the Privacy and Cyber Practice Group. His primary areas of practice are (1) workplace privacy and data security, (2) employee defections, unfair competition, trade secret theft, and corporate espionage, and (3) artificial intelligence.

As co-leader of the firm's Consumer Privacy Team, Usama advises clients on compliance with state consumer privacy laws, including the California Consumer Privacy Act (CCPA), and the California Invasion of Privacy Act. He regularly conducts trainings and publishes articles relating to consumer and employee privacy and data security.

Usama's privacy law experience includes:

- Helping clients achieve full compliance with the CCPA, both as to consumer and employee data.
- Data breach and ransomware triage and response, including advice on compliance with data breach notification laws, drafting data breach notices, and managing company's reporting to law enforcement and government agencies such as attorneys general offices.
- Providing privacy & data security training to managers.
- Defending against invasion of privacy claims, including wiretapping claims based on a website's collection and disclosure of data through cookies, pixels, and other tracking technology.
- Prosecuting litigation against individuals suspected of stealing private information of employees, clients, consumers, and patients, including seeking TRO.
- Advising clients on preventive measures, including, for example, security best practices and vendor contract negotiation/management.

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT, Associate, Fisher & Phillips LLP

Kile Marks counsels clients on data privacy and cybersecurity law and regulations, such as the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Computer Fraud and Abuse Act (CFAA). He is an active member of the firm's Privacy and Cyber practice group and Consumer Privacy Team and advises on and helps manage effective responses to real-time data breaches and drafts and implements comprehensive policy suites for clients ranging from international corporations to small clients.

Marks is a Fellow of Information Privacy (FIP), a Certified Information Privacy Professional (CIPP/US), a Certified Information Privacy Manager (CIPM), a Certified Information Privacy Technologist (CIPT), and a member of the International Association of Privacy Professionals (IAPP).

He has published numerous articles, blogs, and podcasts on cybersecurity rules, information governance, artificial intelligence, the Internet of Things (IoT), attorney general policies, and data breaches.

Prior to joining Fisher Phillips, Marks served as an associate for a global law firm where he focused on data privacy, cybersecurity and information governance matters in Los Angeles, California. His experience also includes time in the consulting industry, in the non-profit sector, with the United States Senate, with the United States Attorney's Office for the District of Columbia and with the United States Air Force as a Cryptologic Language Analyst.