

Alert | Labor & Employment



October 2025

California Expands Whistleblower Retaliation Protections for Employees in the AI Sector

On Sept. 29, 2025, California Gov. Newsom signed [Senate Bill 53](#), the Transparency in Frontier Artificial Intelligence Act, into law. Aimed at preventing catastrophic risks from advanced AI systems, the law sets requirements for large developers working with “frontier models”—including mandatory safety measures, adherence to national and international standards, and public transparency reports. A “frontier model” is defined by the amount of computing power used during training, fine-tuning, or modification—specifically, any model requiring more than 10^{26} integer or floating-point operations.

Violations may lead to civil penalties, especially for failures that might result in mass harm (injury or death of 50 or more people) or financial losses exceeding one billion dollars. The law takes effect Jan. 1, 2026.

Among its provisions, Senate Bill 53 establishes whistleblower protections in the AI sector. Employees involved in risk assessment, safety management, or incident response are expressly shielded from retaliation when reporting violations or disclosing information about critical safety threats. To safeguard those who speak out, legislators of the bill have implemented notice and internal reporting procedures to ensure employees are able to report or disclose information without fear of retaliation.

What Is Considered a Catastrophic Risk?

“Catastrophic risk” is defined as “a foreseeable and material risk that a developer’s development, storage, use or deployment of a frontier model will materially contribute to the death of, or serious injury to, more than 50 people or more than one billion dollars (\$1,000,000) in damage to, or loss of, property arising from a single incident involving a frontier model” doing any of the following:

1. Providing expert level assistance in the creation or release of a chemical, biological, radiological, or nuclear weapon;
2. Engaging in conduct with no meaningful human oversight that is either a cyberattack or, if the conduct had been committed by a human, would constitute the crime of murder, assault, extortion, or theft; and
3. Evading the control of its developer or user.

The statute expressly excludes lawful activity of the federal government, harm caused by a frontier model in combination with other software if the frontier model did not materially contribute to the harm, and information that a frontier model outputs if the information is otherwise publicly accessible in a substantially similar form from another source.

Which Employers Are Covered?

The new law applies to large developers of AI systems that have trained or are training a “frontier model.” It imposes additional requirements on those whose annual gross revenues exceeded \$500 million in the preceding calendar year. While some current models do not reach this high technical threshold, ongoing technological advancements may bring many models above this level in the coming years.

Who Qualifies as an Employee?

Covered employees include any employee responsible for assessing, managing, or addressing risk of critical safety incidents.

Critical safety incidents include the following:

1. Unauthorized access to, modification of, or theft of the model weights of a foundation model that results in death, bodily injury, or damage to property;
2. Harm resulting from a catastrophic risk, which includes events that lead to the death or serious injury of more than 50 people or more than one billion dollars in financial harm;
3. Loss of control of a foundation model causing death or bodily injury; and
4. A foundation model employing deceptive techniques against the frontier developer to subvert the developer’s controls or monitoring—outside of a context of an evaluation designed to elicit this behavior—in a manner that increases catastrophic risk.

Overview of New Whistleblower Protections Statute

Prohibited Conduct

Employers and large developers are prohibited from adopting or enforcing any rule, regulation, policy, or contract that prevents employees from disclosing information about activities posing a catastrophic risk

or violations of the law. Employees are protected if they have reasonable cause to believe the information they disclose reveals such risks or violations, and they may report to the attorney general, federal authorities, persons of authority over employees at their company, or authorized investigators. Cal. Labor Code § 1107.1(a).

Notice and Acknowledgement Requirements

Employers must provide clear notice to all employees about their rights under the law. This includes posting notices in the workplace, notifying new hires, and ensuring remote employees receive equivalent information. Written notice must be provided annually, with employees required to acknowledge receipt. Cal. Labor Code § 1107.1(d).

Internal Reporting Process Requirements

The law requires employers to implement a reasonable internal process for covered employees to anonymously report concerns about catastrophic risks or violations of the new law. Employers must provide monthly updates to the reporting employee on the status of investigations and responsive actions. Summaries of disclosures and responses must be shared with company officers and directors quarterly, except when those individuals are implicated in the alleged wrongdoing. Cal. Labor Code § 1107.1(e).

Consequences for Non-Compliance

Failing to comply may be costly. In addition to the attorney general having sole authority to seek civil penalties up to one million dollars per violation through a civil action, covered employees may also sue if they experience retaliatory adverse employment actions. Covered employees may pursue damages for any harm suffered, injunctive relief, and recovery of attorneys' fees.

Takeaways for Employers

Employers—particularly those developing AI or collaborating with major AI developers—should consider proactively updating internal policies and employee contracts to support safe, protected reporting of critical safety incidents, whether within the organization or to external authorities. Considering California's expansive definitions of "employee" and joint employer liability, AI developers may wish to also ensure that their service providers and contractors adopt compliant practices. This may require a review of not only internal contracts with direct hires but also third-party contracts for consistency with the law's requirements.

Finally, employers may wish to carefully review all adverse actions taken against covered employees to confirm they are not retaliatory. Internal processes may need to be strengthened to safeguard employees who report safety concerns or potential violations.

Authors

This GT Alert was prepared by:

- Kurt A. Kappes | +1 916.868.0650 | kappesk@gtlaw.com
- Timothy Long | +1 916.868.0677 | longt@gtlaw.com
- Noah M. Woo | +1 415.655.1283 | Noah.Woo@gtlaw.com

Abu Dhabi[†]. Albany. Amsterdam. Aspen. Atlanta. Austin. Berlin[‡]. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Dubai[†]. Fort Lauderdale. Houston. Kingdom of Saudi Arabia[¶]. Las Vegas. London^{*}. Long Island. Los Angeles. Mexico City⁺. Miami. Milan[»]. Minneapolis. Munich[‡]. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo[›]. Seoul[∞]. Shanghai. Silicon Valley. Singapore[°]. Tallahassee. Tampa. Tel Aviv[^]. Tokyo[¤]. Warsaw[~]. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. †Greenberg Traurig's Abu Dhabi office is a branch of Greenberg Traurig, P.A., which is registered with the Abu Dhabi Global Market Registration Authority (Registration No. 29906) and licensed to carry out legal services and regulated as a DNFBP by the ADGM Financial Services Regulatory Authority. ‡Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ‹Greenberg Traurig's Dubai office is operated by Greenberg Traurig Limited, a company registered in the Dubai International Financial Centre (Registration No. CL7238), regulated as a DNFBP by the Dubai Financial Services Authority and licensed by The Government of Dubai Legal Affairs Department. ‹Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legali Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ›Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. °Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojijimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2025 Greenberg Traurig, LLP. All rights reserved.*