Insights, News & Events

DON'T DELAY! CALIFORNIA LIKELY TO SOON REQUIRE DATA BREACH NOTIFICATIONS TO BE PROVIDED TO CONSUMERS WITHIN 30 DAYS

Insights
Jul 2, 2025

California may likely soon join the growing list of states to require data breach notifications to be required within a certain amount of time – in this case, 30 calendar days. In recent years, many states have moved to provide specific timeframes for data breach notifications to consumers and regulators, while other states have continued to maintain more flexible deadlines. California lawmakers seem set on establishing a strict and challenging timeframe – what does your business need to know, and how can you prepare?

The Basics

California's proposed legislation (Senate Bill 446) is currently in the state Assembly and currently has no formal opposition reason, it has a strong likelihood of being enacted into law.

- The legislature has until September 12 to pass the measure Governor.
- He will have until October 12 to sign or veto it.
- Should the legislation be signed into law, it will become eff January 1, 2026.

[Ed. Note: Gov. Gavin Newsom signed SB 446 into law on October 3.]

State Data Breach Notifications

In the current national landscape, deadlines for notifying regulators of a data breach for notification to consumers

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132

Benjamin M. Ebbink
Partner
916.210.0400

vary by jurisdiction.

- 29 states plus D.C. and Puerto Rico require notice to consumers "without unreasonable delay."
- The other 21 states require notice to consumers between 30 and 60 days.

These deadlines aim to facilitate faster regulatory oversight, transparency, and public accountability. But they increasingly conflict with the realities of detailed forensic investigations, as it can take weeks (or more) to accurately understand the scope of the incident – and even longer to determine what data was impacted. As states gravitate toward fixed timelines, organizations are under pressure to act quickly, sometimes before they can complete an investigation and have all the facts.

Existing California Data Breach Notification Requirements

Under current law, a California business is required to provide a notification of a data breach to affected individuals "in the most expedient time possible and without unreasonable delay." The notice must require specific formatting guidelines and include required information.

In addition, if the breach involves providing notice to more than 500 California residents, the business must provide a sample copy of the notification to the Attorney General which the Attorney General makes public on its website. There is currently no timeframe associated with the Attorney General notice.

What SB 446 Would Do

Proponents of SB 446 contend that existing California law is vague and does not establish clear notification deadlines for data breaches. They contend that this "loophole" in existing law leaves consumers in the dark about data breaches, compliance is uneven, and enforcement becomes more difficult without a definitive standard. They allege that many notices that are provided to the Attorney General (breaches involving more than 500 California residents) are not reported until more than a year after the data was first accessed, leaving consumers unaware and unable to take timely protective actions.

Therefore, SB 446 provides that consumer data breach notifications must be made within 30 calendar days of

Jillian Seifrit, CIPP/US

Associate

610.230.6129

Service Focus

Data Protection and Cybersecurity

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

discovery or notification of the data breach. Notice to the Attorney General for breaches involving more than 500 Californians must be made within 15 calendar days thereafter.

SB 446 currently maintains existing exemptions and provides that a business may delay the notification to accommodate the legitimate needs of law enforcement (where notification will impede a criminal investigation) or "as necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

However, there are indications that the author of the bill may be planning to amend the bill to delete the permissible delay for "determining the scope of the breach." In 2024, New York amended its data breach notification law to delete exceptions for "determining the scope of the breach" and "restoring the integrity of the data system."

What This Would Mean for California Businesses

SB 446 does not currently have any formal opposition and therefore stands a good likelihood of being enacted into law. If that occurs, California businesses will need to revise their data breach processes to ensure that notice is provided to consumers within 30 calendar days unless a covered exemption applies.

Revised Processes

This could also raise the stakes for California businesses. The 30-day notification deadline presents a significant challenge to compliance efforts, particularly when lengthy and detailed forensic investigations are required to determine the scope of the incident and the data impacted. This rigid timeline can force employers to issue premature or incomplete notifications, which may confuse their employees and undermine trust.

Strict Violations

If SB 446 is enacted, any failure to provide required notice within the 30 calendar-day period could be used as "per se" evidence of a violation of the law. Further, under California law, businesses regulated by the California Consumer Privacy Act (CCPA) can face both regulatory fines and a private right of action for data breaches resulting from a

business's failure to implement reasonable security measures.

Hefty Fines

As of 2025, the regulatory fines range from not more than $2,663 for each violation or $7,988 for each intentional violation and violations involving the personal information of consumers whom the violator has actual knowledge are under 16 years of age. In the context of data breaches, even if an employer doesn't hire consumers under 16, employers may have the data of employees' dependents on their systems, which could potentially subject them to fines in the event of a breach impacting that data.

Civil Lawsuits

Additionally, California law provides a private right of action. This allows for consumers to recover damages of not less than $107 and not greater than $799 per consumer per incident or actual damages, whichever is greater.

What Should You Do?

California businesses should continue to monitor the status of SB 446 and any further amendments, although as stated above the bill appears likely to be enacted into law and effective next year.

- Of course, the best way to avoid having to comply with any specific data breach notification requirement is to avoid a data breach in the first place. Therefore, California businesses should redouble their safety and security protocols to ensure that consumer and employee data is properly safeguarded.
- In addition, to prepare for the likely enactment of SB 446, businesses should be prepared to update incident response plans as necessary to ensure adherence to the new deadlines, in the event of an incident that would require notice.
- Finally, businesses should make plans to implement an internal process and procedure to ensure compliance with the potential more specific timeframe, including building systems for prompt communication regarding data breaches from any third-party vendors.

Conclusion

Fisher Phillips will continue to monitor developments regarding this proposed legislation and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the author of this Insight, or any member of our Data Protection and Cybersecurity Team or an attorney in our California offices for guidance and support.