Date of Hearing: June 24, 2025
Fiscal: No

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 446 (Hurtado) – As Amended May 14, 2025

SENATE VOTE: 39-0

SUBJECT: Data breaches: customer notification

SYNOPSIS

California's data breach notification laws require government agencies, individuals, and businesses to notify residents when their personal information may have been accessed by an unauthorized party. These laws are intended to ensure timely notification so that consumers can take steps to protect their personal information and guard against identity theft.

However, current law has proven insufficient, as it only requires that notices be made "in the most expedient time possible and without unreasonable delay." This vague standard has resulted in significant delays, with some data breaches being reported to consumers and the Attorney General months—or even years—after the breach occurred.

This author-sponsored bill strengthens California's notification requirements by mandating that individuals and businesses disclose a breach to affected consumers within 30 calendar days of discovering or being notified of it. The bill includes reasonable flexibility, allowing delays if required for legitimate law enforcement purposes or to determine the full scope of the breach. Additionally, if a breach affects more than 500 consumers, it must be reported to the Attorney General within 15 days of notifying consumers. This bill is supported by Oakland Privacy and Secure Justice.

If passed by this Committee, the bill will next be heard by Assembly Judiciary Committee.

THIS BILL:

1) Requires an individual or business to provide the relevant data breach disclosure within 30 calendar days of discovery or notification of the data breach. A business may delay the disclosure to accommodate the legitimate needs of law enforcement or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

2) Requires an individual or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system to electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General within 15 calendar days of notifying affected consumers of the security breach.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Establishes the Information Practices Act of 1977, which declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. Further states the following legislative findings:

   a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies;

   b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and

   c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798 et seq.)

3) Establishes the California Customer Records Act, which provides requirements for the maintenance and disposal of customer records and the personal information contained therein. (Civ. Code § 1798.80 et seq.) Further states it is the intent of the Legislature to ensure that personal information about California residents is protected and to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information. (Civ. Code § 1798.81.5(a).)

4) Requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure, and to contractually require nonaffiliated third parties to which it discloses such personal information to similarly protect that information. (Civ. Code § 1798.81.5.)

5) Establishes the Data Breach Notification Law, which requires any agency, person, or business that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made promptly after the law enforcement agency determines that it will not compromise the investigation. (Civ. Code §§ 1798.29(a), (c) & 1798.82(a), (c).)

6) Requires, pursuant to the Data Breach Notification Law, any agency, person, or business that maintains computerized data that includes personal information that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code §§ 1798.29(b), 1798.82(b).)

7) Defines "personal information," for the purposes of the data breach notification law, to mean either of the following:

   a) An individual's first name or first initial and the individual's last name in combination with one or more specified data elements, such as social security number, medical information, health insurance information, credit card number, or unique biometric, when either the name or the data elements are not encrypted or redacted; or

   b) A username or email address in combination with a password or security question and answer that would permit access to an online account. (Civ. Code §§ 1798.29(g) and (h); 1798.82(h) & (i).)

8) Provides that an agency, person, or business that is required to issue a security breach notification shall meet specified requirements. The notification must be written in plain language, meet certain type and format requirements, be titled "Notice of Data Breach," and include specified information. (Civ. Code §§ 1798.29(d), 1798.82(d).) Authorizes the entity to also include in the notification information about what it has done to protect individuals whose information has been breached or advice on steps that the person may take to protect themselves. (Civ. Code §§ 1798.29(d), 1798.82(d).)

COMMENTS:

1) **Author's statement**. According to the author:

> Cybersecurity breaches continue to threaten the personal and financial security of Californians, exposing sensitive data and leaving individuals vulnerable to identity theft and fraud. While existing law requires entities to report data breaches affecting more than 500 residents, it lacks a specific deadline for disclosure. As a result, affected individuals may not be informed for months—or even a year—delaying their ability to take preventive measures.
>
> SB 446 strengthens consumer protections by establishing clear notification timelines for security breaches. Under this bill, businesses and organizations must notify affected individuals within 30 days of a breach and also provide a copy to the California Attorney General within 15 days after. This ensures timely awareness, allowing people to secure their personal information and mitigate potential harm.
>
> By closing a critical loophole in California's data protection laws, SB 446 upholds transparency and accountability while ensuring that residents are not left in the dark about threats to their data. Californians deserve the right to act swiftly when their personal information is compromised, and this bill provides the necessary framework to protect them.

2) **The Rise in Data Breaches.** As California's economy and the lives of its residents become increasingly digitized, the volume of data collected and stored by various entities continues to grow. Yet, as consumers shift more of their transactions and interactions online, they are growing wary of what information is collected about them and how it is used. In 2023, the Pew Research Center found that 81% of U.S. adults are concerned about how companies use their data, and 61% are skeptical that any privacy safeguards they take will meaningfully limit how

companies collect that information.[1] These concerns are compounded by the risk that such data may be stolen or leaked in a breach, leaving consumers exposed.

As the Electronic Privacy Information Center describes:

> The more data companies collect about us, the more our data is at risk. When companies hold your data, the greater the odds it will be exposed in a breach or a hack and end up in the hands of identity thieves, scammers, or shadowy companies known as data brokers that buy and sell a huge amount of data about Americans.[2]

The private sector has done little to ease public concerns. In February 2024, it was revealed that Change Healthcare suffered a massive data breach impacting over 100 million people.[3] The breach, carried out via a ransomware attack, exploited a system protected by only a single password, without even basic safeguards like multifactor authentication. That a company earning $22 billion in 2023 had such poor cybersecurity raises serious questions about the safety of consumer data across the corporate landscape, particularly among companies with fewer resources.

Earlier this year, Blue Shield of California was reported to have leaked data from 4.7 million members to Google.[4] Although Blue Shield had intentionally shared website usage data with Google for targeted advertising, it was discovered that for three years, it had inadvertently shared sensitive health information as well. Google was thus able to use this health data, intended to be private, for its own purposes, including ad targeting. This was not just a data breach, but a profound breach of trust. The public expects health data to remain confidential, yet Blue Shield's negligence compromised the health information of more than 10% of California's population over an extended period.

These are just two recent examples, but they reflect a broader trend. In 2025 alone, the California Attorney General's office has received notices of over 240 data breaches, each affecting more than 500 residents.[5] Alarmingly, many of these breaches were not reported until more than a year after the data was first accessed, leaving consumers unaware and unable to take timely protective actions like changing passwords or deleting compromised accounts.

Under California's Data Breach Notification Law, any person or business that owns or licenses computerized data containing personal information must notify any affected California resident when unencrypted personal data is, or is reasonably believed to have been, acquired by an

---

[1] Colleen McClain et al., "Views of data privacy risks, personal data and digital privacy laws", *Pew Research Center* (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/.
[2] Caitriona Fitzgerald, Kara Williams, and R.J. Cross, "The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better", *Electronic Privacy Information Center* (Feb. 2024), https://epic.org/documents/the-state-of-privacy-report/.
[3] Steve Adler, "UnitedHealth Adopts Aggressive Approach to Recover Ransomware Attack Loans", *The HIPAA Journal* (Apr. 16, 2025).
[4] Zack Whittaker, "UnitedHealth says Change Healthcare hack affects over 100 million, the largest-ever US healthcare data breach", *Tech Crunch* (Oct. 24, 2024), https://techcrunch.com/2024/10/24/unitedhealth-change-healthcare-hacked-millions-health-records-ransomware/.
[5] The data breach data base can be found at https://oag.ca.gov/privacy/databreach/list.

unauthorized party.[6] These notifications must be titled "Notice of Data Breach," follow specific formatting guidelines, and include required information. This legal requirement is intended to ensure that consumers are informed quickly so they can take necessary steps to protect themselves, such as changing passwords, monitoring financial accounts, or freezing credit.

Although the law allows for a delay in notification if required by law enforcement, many breaches are still not reported promptly. This delay undermines the purpose of the law and puts consumers' privacy and security at even greater risk.

3) **What this bill would do.** This bill seeks to ensure that data breaches are reported in a timely manner, empowering consumers to take reasonable steps to protect themselves after their personal information has been compromised. Specifically, it would require that data breach notifications be sent to affected individuals within 30 days of the breach being identified. The bill allows flexibility if the investigation into the breach takes longer than 30 days. It also maintains existing provisions that permit a business to delay notification to accommodate legitimate law enforcement needs or to determine the scope of the breach and restore the reasonable integrity of the data system.

In addition, the bill provides that any person or business required to issue a security breach notification to more than 500 California residents as a result of a single breach must electronically submit a sample copy of that notification—excluding any personally identifiable information—to the Attorney General. This submission must be made within 15 calendar days of notifying affected consumers.

ARGUMENTS IN SUPPORT: Oakland Privacy writes in support:

> Timely data breach notifications are the backbone of effective privacy laws. Ambiguous timelines, such as "the most expedient time possible and without unreasonable delay," fail to adequately give clear notice about what constitutes conformance. As long as a delay can be argued as "reasonable," businesses may exercise discretion in interpreting these inexact timelines to their advantage and at the expense of consumers.
>
> As a result, compliance becomes uneven, enforcement becomes more difficult without a definitive standard, and consumers remain vulnerable to preventable harm.
>
> Laws should provide clear, enforceable standards so that businesses fully understand their obligations and regulators can administer accountability consistently. Defined notification timelines prevents businesses from delaying disclosures for reputational or financial reasons. Swift disclosure allows individuals to take immediate protective measures, such as freezing credit or monitoring their accounts. Delayed notifications increase the risk of identity theft, financial fraud, and consumer harm.
>
> The parameters of privacy laws should not be open to interpretation when the stakes are so high. Establishing delineated notification timelines improves business accountability, enhance regulatory enforcement, and strengthens consumer protection. Updating existing law with SB446 will affirm California's leadership in privacy, cybersecurity, and consumer protection standards.

---

[6] Civ. Code §§ 1798.29(a), (c) &1798.82(a), (c).

For these reasons, Oakland Privacy supports SB 446 and urges you to pass the bill onwards.

ARGUMENTS IN OPPOSITION: None on file.

REGISTERED SUPPORT / OPPOSITION:

Support

California Police Chiefs Association
Consumer Attorneys of California
Oakland Privacy
Privacy Rights Clearinghouse
Secure Justice

Opposition

None on file

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200