Date of Hearing: July 8, 2025

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 446 (Hurtado) – As Amended May 14, 2025

PROPOSED CONSENT

SENATE VOTE: 39-0

SUBJECT: DATA BREACHES: CUSTOMER NOTIFICATION

KEY ISSUE: SHOULD CALIFORNIA STRENGTHEN ITS DATA BREACH NOTIFICATION LAW BY IMPOSING SPECIFIC DEADLINES TO NOTIFY AFFECTED INDIVIDUALS AND THE ATTORNEY GENERAL, IN ORDER TO REDUCE HARMFUL DELAYS AND ENSURE TIMELY DISCLOSURE OF CYBERSECURITY INCIDENTS?

SYNOPSIS

California law currently requires entities that experience a data breach affecting more than 500 residents to notify both the affected individuals and the Attorney General. However, the statute does not specify a fixed deadline for when these notifications must occur. As a result, organizations may legally delay disclosures for extended periods, even when the compromised data includes sensitive personal information such as usernames, passwords, or financial credentials. This lack of temporal clarity undermines the law's consumer protection purpose by leaving individuals unaware of ongoing threats and unable to take timely protective measures such as updating login credentials, placing credit freezes, or monitoring financial accounts for fraudulent activity. SB 446 directly addresses this deficiency by imposing firm, enforceable deadlines: entities must notify affected individuals within 30 days of discovering a breach and provide a copy of that notice to the Attorney General within 15 days thereafter.

This measure has no opposition on file, and is supported by organizations such as the Consumer Attorneys of California, Oakland Privacy, and the California Police Chiefs Association. The bill previously passed the Assembly Committee on Privacy & Consumer Protection on consent.

SUMMARY: Requires that consumers be notified of a data breach within 30 days of its discovery and mandates submission of notices affecting more than 500 Californians to the Attorney General within 15 days of notifying the consumers of the breach. Specifically, **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.

2) Provides that 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.

3) 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. (California Constitution, Article I, Section 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. (Civil Code Section 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. (Civil Code Section 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. (Civil Code Section 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. (Civil Code Section 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. (Civil Code Sections 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. (Civil Code Sections 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. (Civil Code Sections 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. (Civil Code Sections 1798.29 (d), 1798.82 (d).)

9) Authorizes the entity to also include in the notification information described in 8) what it has done to protect individuals whose information has been breached or advice on steps that the person may take to protect themselves. (Civil Code Sections 1798.29 (d), 1798.82 (d).)

FISCAL EFFECT: As currently in print this bill is keyed non-fiscal.

COMMENTS: California law currently requires entities that experience a data breach affecting more than 500 residents to notify both the affected individuals and the Attorney General. However, the statute does not specify a fixed deadline for when these notifications must occur. As a result, organizations may legally delay disclosures for extended periods, even when the compromised data includes sensitive personal information such as usernames, passwords, or financial credentials. This lack of temporal clarity undermines the law's consumer protection purpose by leaving individuals unaware of ongoing threats and unable to take timely protective measures such as updating login credentials, placing credit freezes, or monitoring financial accounts for fraudulent activity. SB 446 directly addresses this deficiency by imposing firm, enforceable deadlines: entities must notify affected individuals within 30 days of discovering a breach and provide a copy of that notice to the Attorney General within 15 days thereafter.

As explained by 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 or more later—delaying their ability to take preventive measures.

> The absence of a required notification timeline not only delays protective actions but also reduces accountability for organizations handling sensitive data. Without a legal deadline in place, businesses and institutions may deprioritize prompt disclosures, either unintentionally or to limit reputational damage.
>
> SB 446 strengthens consumer protections by establishing clear notification timelines for cybersecurity 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 limit potential harm. This will not only protect consumers but also encourage organizations to improve their cybersecurity measures and response plans.
>
> 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.

"Notice of Data Breach." As California's economy becomes increasingly digitized, the volume of personal data collected, stored, and transmitted by both private and public entities has grown exponentially. Californians now conduct much of their daily activity online—including banking, shopping, healthcare access, and employment. As digital activity increases, so too does the incentive for companies to collect, track, and monetize user data—often with minimal transparency or consent. This environment has led to significant consumer concern. 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 privacy measures they take will meaningfully restrict data collection. (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/.)

These concerns are heightened by the ever-growing risk of data breaches. As the Electronic Privacy Information Center (EPIC) has noted:

> 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.

(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/.)

The consequences of these breaches are not theoretical—they are playing out in real time. In February 2024, a ransomware attack on Change Healthcare compromised the data of over 100 million individuals. Investigations revealed that the breach was enabled by shockingly weak security protocols: a critical system was protected by a single password and lacked basic protections like multifactor authentication. (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/.) Despite earning $22 billion in revenue the previous year, Change Healthcare failed to implement even baseline safeguards, raising concerns

about the vulnerability of consumer data across the corporate sector—particularly among entities with fewer resources.

Similarly, in 2024, Blue Shield of California admitted to sharing data from 4.7 million members with Google through a misconfigured analytics tool. Although intended for website optimization, the tool captured and transmitted sensitive health information, which Google then used for advertising purposes. The disclosure spanned three years and affected more than 10% of California's population. While not a traditional breach by an external attacker, the incident demonstrated how negligence in data handling can expose confidential health data and violate consumer trust. (Aimee Picchi, *Blue Shield of California Exposed Data of 4.7 Million Patients to Google for Years*, Yahoo! Finance (Mar. 5, 2024), https://finance.yahoo.com/news/blue-shield-california-exposed-data-115539774.html.)

Alarmingly, many of these breaches were not disclosed until months—or even more than one year—after they occurred. For example, the Natomas Unified School District discovered in July 2024 that it had suffered a cybersecurity breach compromising the usernames and passwords of 14,500 students. The district waited six months before notifying families and the Attorney General, a delay that—while technically permissible under current law—left students and their families exposed without the opportunity to protect themselves. (Jennah Pendleton, *A Sacramento school district waited months to disclose a data breach. What info was exposed*, The Sacramento Bee (Jan. 15, 2025), https://www.sacbee.com/news/local/education/article298476538.html#storylink=cpyhttps://www.sacbee.com/news/local/education/article298476538.html.)

Existing law. Under California's existing Data Breach Notification Law (Civil Code Section 1798.82), any person or business that owns or licenses computerized data containing personal information must notify affected California residents if unencrypted data is, or is reasonably believed to have been, acquired by an unauthorized party. If the breach affects more than 500 residents, the business must also submit a sample of the consumer notice to the Attorney General (Civil Code Section 1798.82 (f)). These notices must be labeled as a "Notice of Data Breach" and follow specific formatting and content requirements. The intent is to give consumers timely and actionable information to safeguard their accounts, change passwords, and monitor financial activity.

However, the statute currently does not specify a firm deadline for such notifications, aside from limited delay for law enforcement needs. In practice, this has led to long delays in breach disclosure, undermining the statute's protective function. Without a deadline, entities may delay notification to mitigate reputational harm or out of administrative inertia, leaving consumers unaware and unprotected. Given the scale of data collection and the frequency with which California is targeted—in 2021, the state led the nation in breaches, with over 67,000 victims losing more than $1.2 billion (Fed. Bureau of Investigation, *2021 Internet Crime Report*, Internet Crime Complaint Center, at pp. 26-27 (Feb. 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)—this legal gap is untenable.

This bill. SB 446 seeks to address this gap by imposing clear, enforceable deadlines for breach notification—ensuring that affected individuals receive timely alerts and that entities face meaningful accountability when consumer data is compromised. Specifically, SB 446 would require that individuals affected by a data breach receive notice within 30 calendar days of the

breach being identified. The bill sets a clear standard for timely notification while allowing for reasonable extensions if the breach investigation takes longer than 30 days. It also preserves existing provisions that permit delay when necessary to accommodate law enforcement needs, determine the full extent of the breach, or restore the security of the affected system.

Additionally, the bill would require any person or business that notifies more than 500 California residents of a single breach to submit an electronic copy of the notification—excluding any personally identifiable information—to the Attorney General. This submission must occur within 15 days of notifying affected consumers.

ARGUMENTS IN SUPPORT: The California Police Chiefs Association explains its support of SB 446:

> In an era where cybercrime and data theft are increasingly sophisticated, the provisions in SB 446 address the urgent need for timely and transparent disclosure to those affected by breaches of sensitive information. By mandating that entities notify affected individuals within 30 calendar days of discovering a breach, the bill empowers Californians to take prompt protective action—such as freezing credit, changing passwords, or monitoring their identities—thereby limiting further harm.
> Importantly, SB 446 strikes a thoughtful balance by maintaining essential provisions that allow for delayed notifications at the request of law enforcement if public disclosure could impede ongoing criminal investigations. This respect for investigative integrity ensures that our ability to pursue cybercriminals is preserved while also protecting the public interest.

Privacy Rights Clearinghouse also supports this measure:

> Each year, thousands of Californians have their personal data compromised, yet many do not find out until months or even a year later. Existing law mandates that any data breach affecting more than 500 California residents be reported to both the affected individuals and the Office of the Attorney General. However, the statute does not establish a specific deadline for disclosure, resulting in significant delays that leave consumers vulnerable. In some cases, individuals may not receive notification of a breach for several months or even a year, impeding their ability to take timely protective measures.
>
> Current law recognizes that it is important to inform individuals of these security breaches but does not provide a required timeline to do so. Establishing a firm timeline on when to notify the Attorney General, as well as any individual, of a breach in security of their personal information is vital to keeping California's consumers safe and protected online. SB 446 expands on existing law by requiring individuals and businesses to notify the Office of the Attorney General within 15 calendar days of notifying affected individuals of a security breach and inform affected individuals within 30 calendar days. SB 446 does not change existing thresholds of when notification is required. Implementing an actual time period informs individuals about the status of their personal data in a timely manner so they may take necessary actions to safeguard their livelihood.

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: Shiran Zohar / JUD. / (916) 319-2334