SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 446 (Hurtado)
Version: February 18, 2025
Hearing Date: April 1, 2025
Fiscal: No
Urgency: No
CK

SUBJECT

Data breaches: customer notification

DIGEST

This bill requires data breach disclosures to be made to California residents within 30 days, except as specified. This bill requires a copy of the disclosure to be delivered to the Attorney General within 15 days.

EXECUTIVE SUMMARY

California's data breach notification statutes require government agencies, persons, and businesses to provide residents with specified notices in the wake of breaches of residents' personal information. The goal of such laws is to provide timely notice to consumers, enabling them to, among other things, take steps to protect their personal information and to prevent identity theft.

Concerns have been raised about the law's indefinite timeline. Currently the law provides that breach notifications should be made in the "most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

This bill instead requires individuals or business to provide breach disclosures within 30 calendar days of discovery or notification of the data breach. However, it continues to provide flexibility by allowing businesses to delay 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." To ensure some oversight, large data breaches must be disclosed to the Attorney General within 15 days. This bill is author-sponsored. No timely support or opposition has been received by the Committee.

PROPOSED CHANGES TO THE LAW

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, Sec. 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. It 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.) It 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 shall be made promptly after the law enforcement agency determines that it will not compromise the investigation. (Civ. Code §§ 1798.29(a), (c) and 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) Provides that a person 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 shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.

8) 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) and (i).)

9) 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).) Additionally, it authorizes them, in their discretion, to also include in the notification information about what the person or business 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).)

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.[1]

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 discovery or notification of the security breach.

COMMENTS

1. The stunning incidence of data breaches

A vast majority of Californians engage in a wide range of activities online. Even before the pandemic forced many people to drastically shift their lives online, 70 percent of people in the state received financial services online, 39 percent telecommuted, 42 percent accessed sensitive health or insurance records online, and 39 percent communicated with doctors.[2] In addition, many companies have realized the financial benefits of collecting as much data on consumers as possible, tracking, storing, and selling the details of our everyday lives. Given the amount of activity online and the massive amount of data being collected and switching hands, concerns about data security have skyrocketed.

Unfortunately, because of the size of California's economy and the sheer number of consumers, the data collected and held by California businesses is frequently targeted by cyber criminals, and California accounts for a sizeable share of the nation's data breaches.[3] According to reports, California led the nation in data breaches between 2017-2021, with 325,291 victims losing more than $3.7 billion.[4] According to the

[1] The bill currently applies this provision to only businesses. The author has agreed to an amendment that applies this to individuals and businesses.
[2] Niu Gao & Joseph Hayes, *California's Digital Divide* (February 2021) Public Policy Institute of California, https://www.ppic.org/publication/californias-digital-divide/. All internet citations are current as of March 21, 2025.
[3] California Department of Justice, *California Data Breach Report* (February 2016) https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[4] Kevin Smith, *California leads the nation in data breaches* (July 25, 2022) Orange County Register, https://www.ocregister.com/2022/07/25/california-leads-the-nation-in-data-breaches/.

Attorney General's Office, there have been over 2,200 reported data breaches since the start of 2021 alone.

The frequency of data breaches in California and the threat that such breaches pose make the enactment and enforcement of statutes protecting against and responding to these breaches vital to maintaining the right to privacy for California residents. California has addressed these issues over the years by requiring specific procedures for notifying individuals of data breaches and requiring certain security procedures and practices to prevent such breaches.

2. Laws to respond to data breaches

In 2003, California's first-in-the-nation security breach notification law went into effect. (*See* Civ. Code §§ 1798.29, 1798.82.) Since that time, almost all states have enacted similar security breach notification laws, and governments around the world have or are considering enacting such laws. There are two provisions governing data breach notification requirements, Civil Code Sections 1798.29 and 1798.82. The two provisions are nearly identical, but the former applies to public agencies and the latter, relevant here, to persons or businesses.

California's data breach notification law requires any 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. Such breach notifications must be titled "Notice of Data Breach," are required to meet certain formatting requirements, and must include specific information. This notification requirement ensures that residents are made aware of a breach, thus allowing them to take appropriate action to mitigate or prevent potential financial losses due to fraudulent activity such as changing passwords, monitoring accounts, or placing credit freezes.

Relevant here, 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. With regard to the law enforcement provision, the notification required 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.

Concerns have been raised that this indefinite timeline for providing consumers notice of a breach is undermining the goals of the law and that businesses are improperly delaying disclosure. This bill therefore requires the disclosure to be made to relevant California residents within 30 calendar days of discovery or notification of the data breach. However, the bill continues to provide flexibility to ensure notification does not impede criminal investigations or the ability of a business to shore up the breached

system before publicly announcing it. The bill continues to provide that a business may delay the disclosure required to accommodate the legitimate needs of law enforcement, as currently provided, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

However, the bill requires timely notice still be provided to the Attorney General. Currently a person or business that is required to issue a security breach notification pursuant to the data breach notification law to more than 500 California residents as a result of a single breach of the security system must electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. This bill provides that the notice must be issued to the Attorney General within 15 calendar days of discovery or notification of the security breach.

Some concerns have been raised by industry regarding these changes. They highlight that 15 days is generally not enough time to adequately assess even the basic details of a breach and certainly not always enough time to know with certainty whether it has affected more than 500 Californians. They argue that this will likely lead to an over reporting to the Attorney General, creating inefficiencies and potentially misplaced panic amongst the public in certain situations.

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 the California Attorney General within 15 days of a breach and inform affected individuals within 30 days. 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.

SUPPORT

None received

OPPOSITION

None received

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

AB 825 (Levine, Ch. 527, Stats. 2021) amended the definition of "personal information" in the data breach notification law to include "genetic information."

AB 1130 (Levine, Ch. 750, Stats. 2019) amended the definition of "personal information" in the data breach notification law to include biometric information, as specified, as well as certain government identification numbers.

****