AMENDED IN SENATE MAY 14, 2025

AMENDED IN SENATE APRIL 3, 2025

# SENATE BILL No. 446

**Introduced by Senator Hurtado**

February 18, 2025

An act to amend Section 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 446, as amended, Hurtado. Data breaches: customer notification.

Existing law requires an individual or a business that conducts business in California, and that owns or licenses computerized data that includes personal information, to disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was compromised, as specified, and requires that disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

This bill would require that data breach disclosure to be made within 30 calendar days of discovery or notification of the data breach but would authorize an individual or business to delay the disclosure to accommodate the legitimate needs of law enforcement, as specified, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Existing law also requires an individual or business that is required to issue the security breach notification described above 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.

This bill would require that submission to the Attorney General to be made within 15 calendar days of ~~discovery or notification~~ *notifying affected consumers* of the security breach.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

*The people of the State of California do enact as follows:*

SECTION 1. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) (1) An individual or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person, and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.

(2) (A) Subject to subparagraph (B), the disclosure required by this subdivision shall be made within 30 calendar days of discovery or notification of the data breach.

(B) An individual or business may delay the disclosure required by this subdivision to accommodate the legitimate needs of law enforcement, pursuant to subdivision (c), or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) An individual or business that maintains computerized data that includes personal information that the individual or business does not own shall notify the owner or licensee of the information

of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) An individual or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What ~~Happened,"~~ *Happened?"* "What Information Was ~~Involved,"~~ *Involved?"* "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

| | |
|---|---|
| [NAME OF INSTITUTION / LOGO] | Date: [insert date] |
| NOTICE OF DATA BREACH | |
| | |

| | |
|---|---|
| What Happened? | |
| What Information Was Involved? | |
| What We Are Doing. | |
| What You Can Do. | |
| Other Important Information.<br>[insert other important information] | |
| For More Information. | Call [telephone number] or go to [internet website] |

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting individual or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the individual or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected individual for not less than 12 months along with all information necessary to take advantage of the offer to any individual whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the individual or business, the security breach notification may also include any of the following:

(A) Information about what the individual or business has done to protect individuals whose information has been breached.

(B) Advice on steps that people whose information has been breached may take to protect themselves.

(C) In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) An individual or business that is required to issue a security breach notification pursuant to this section 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 within 15 calendar days of ~~discovery or notification of~~ *notifying affected consumers of* the security breach. A single sample copy of a security breach notification shall not be deemed to be within Article 1 (commencing with Section 7923.600) of Chapter 1 of Part 5 of Division 10 of Title 1 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the individual or business. Good faith acquisition of personal information by an employee or agent of the individual or business for the purposes of the individual or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(H) Genetic data.

(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person

through a security technology or methodology generally accepted in the field of information security.

(5) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the individual or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the individual or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the individual or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the individual or business, if the individual or business maintains one. For purposes of this subparagraph, conspicuous posting on the individual's or business's internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined

in paragraph (1) of subdivision (h), the individual or business may comply with this section by providing the security breach notification in electronic or other form that directs the individual whose personal information has been breached promptly to change the individual's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the individual or business and all other online accounts for which the individual whose personal information has been breached uses the same username or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the individual or business, the individual or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the individual or business knows the resident customarily accesses the account.

(k) For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render data usable, readable, and decipherable.

(*l*) Notwithstanding subdivision (j), ~~a~~ *an* individual or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this ~~part,~~ *part* shall be deemed to be in compliance with the notification requirements of this section if the individual or business notifies subject individuals in accordance with its policies in the event of a breach of security of the system.

O