AMENDED IN ASSEMBLY MARCH 26, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 964

Introduced by Assembly Member Chau

February 26, 2015

An act *to amend Section 1798.82 of the Civil Code,* relating to civil law.

LEGISLATIVE COUNSEL'S DIGEST

AB 964, as amended, Chau. Civil law: privacy.

Existing law requires a person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, a breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. *Existing law requires the disclosure to 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 would ~~state the intent of the Legislature to enact legislation to protect the public from data breaches.~~ *instead require the disclosure to be made within 30 days, consistent with the legitimate needs of law enforcement.*

The bill would authorize the Attorney General to grant a person or business an additional period of time, not exceeding 30 days, in which to make the disclosure if the Attorney General determines that the person or business needs additional time in order to determine the scope of

the security breach, prevent further disclosures, conduct a risk assessment, restore the integrity of the data system, or provide notice to an entity designated to receive reports and information about information security incidents.

The bill would also provide that if the data containing personal information was encrypted, as defined, there would be a presumption that a breach of the security of the data does not compromise the security, confidentiality, or integrity of the personal information, and no disclosure would be required. That presumption would be rebuttable in a civil action against a person or business for failure to comply with these provisions by facts demonstrating that in the present instance, the security technologies or methodologies used to encrypt the data have been, or are reasonably likely to have been, compromised.

Vote: majority. Appropriation: no. Fiscal committee: ~~no~~ *yes*. 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)* A person 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~~ *notification, pursuant to subdivision (b),* 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. The disclosure shall be made in the most expedient time possible and ~~without unreasonable delay,~~ *within 30 days,* consistent with the legitimate needs of law enforcement, as provided in subdivision ~~(c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.~~ *(c).*

(2) If the data containing personal information was encrypted, there shall be a presumption that a breach of the data does not comprise the security, confidentiality, or integrity of the personal information contained therein, and no disclosure is required. That presumption shall be rebuttable in a civil action pursuant to subdivision (b) of Section 1798.84 against a person or business for failure to make the required disclosure by facts demonstrating

that in the present instance the security technologies or methodologies used to encrypt the data have been, or are reasonably likely to have been, compromised and disclosure is required in accordance with paragraph (1).

(3) If a person or business requires additional time to disclose a breach, it shall provide the Attorney General records or other evidence demonstrating the need to delay disclosure. If the Attorney General determines that the person or business needs additional time in order to determine the scope of a security breach, prevent further disclosures, conduct a risk assessment, restore the integrity of the data system, or provide notice to an entity designated to receive reports and information about information security incidents, threats, and vulnerabilities, it may grant the person or business an additional period of time, not exceeding 30 days, in which to make the disclosure. The Attorney General shall grant additional time to make the disclosure in writing specifying the amount of additional time granted.

(b) A person or business that maintains computerized data that includes personal information that the person 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) A person 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.

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

(A) The name and contact information of the reporting person 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 *pursuant to paragraph (3) of subdivision (a) or* 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 person 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 person for not less than 12 months, along with all information necessary to take advantage of the offer to any person 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 person or business, the security breach notification may also include any of the following:

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

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(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 person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the

person whose personal information has been breached uses the same user name 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 person or business, the person 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 subdivision (j) 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 person or business knows the resident customarily accesses the account.

(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) A person 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. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 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 person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person 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 or California identification card number.

(C) Account number, 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.

(2) A user name 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 through a security technology or methodology generally accepted in the field of information security.

(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 person 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 person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

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

(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(k) Notwithstanding subdivision (j), a person 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, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

~~SECTION 1. It is the intent of the Legislature to enact legislation to protect the public from data breaches.~~

O