Assembly Bill No. 1859

CHAPTER 532

An act to add Section 1798.81.6 to the Civil Code, relating to information privacy.

[Approved by Governor September 19, 2018. Filed with Secretary of State September 19, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1859, Chau. Customer records.

Existing law regulating consumer credit reporting agencies provides as its purpose to require, among other things, that these agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit in a manner that is fair and equitable to the consumer with regard to the confidentiality of such information and in a manner that will best protect the interests of the people of the state. Existing law requires a person or business that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any 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 agency 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 useable. Existing law requires the disclosure to be made in the most expedient time possible and without unreasonable delay, as specified. Existing law authorizes any customer who is injured by a violation of these provisions to institute a civil action to recover damages.

This bill would require a consumer credit reporting agency that owns, licenses, or maintains personal information about a California resident, or a 3rd party that maintains personal information about a California resident on behalf of a consumer credit reporting agency, that knows, or reasonably should know, that a computer system it owns, operates, or maintains, and for which it controls the security protocols, is subject to a security vulnerability that poses a significant risk to the security of computerized data within the system that contains personal information, to take certain measures to protect that data, including implementing software updates, if it knows or reasonably should know that a software update is available to address the security vulnerability, and employing reasonable compensating

controls to reduce the risk of a breach caused by computer system vulnerability until the software update is complete, as specified.

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

SECTION 1. Section 1798.81.6 is added to the Civil Code, to read:

1798.81.6. (a) A consumer credit reporting agency, as defined in 15 U.S.C. Sec. 1681a(p), that owns, licenses, or maintains personal information about a California resident, or a third party that maintains personal information about a California resident on behalf of a consumer credit reporting agency, that knows, or reasonably should know, that a computer system it owns, operates, or maintains, and for which it controls the security protocols, is subject to a security vulnerability that poses a significant risk, as defined in subdivision (c), to the security of computerized data that contains personal information, as defined in subdivision (h) of Section 1798.82, shall do all of the following:

(1) If a consumer credit reporting agency knows or reasonably should know that a software update is available to address the vulnerability as described in subdivision (a), the agency shall begin the necessary testing, planning, and assessment of its systems for implementation of that software update in the most expedient time possible and without unreasonable delay, in keeping with industry best practices, but in any case no later than three business days after becoming aware, or after the point at which it reasonably should have become aware, of the vulnerability and the available software update. The software update shall be completed in the most expedient time possible and without unreasonable delay, in keeping with industry best practices, but in any case no later than 90 days after becoming aware, or after the point at which it reasonably should have become aware, of the vulnerability and the available software update.

(2) Until the software update described in paragraph (1) is complete, the consumer credit reporting agency shall, in keeping with industry best practices, employ reasonable compensating controls to reduce the risk of a breach caused by computer system vulnerability as described in subdivision (a).

(b) Notwithstanding whether a software update is available, the consumer credit reporting agency, in keeping with industry best practices, shall do all of the following:

(1) Identify, prioritize, and address the highest risk security vulnerabilities most quickly in order to reduce the likelihood that the vulnerabilities that pose the greatest security risk will be exploited.

(2) Test and evaluate the impact of compensating controls and software updates and how they affect the vulnerability of the system to threats to the security of computerized data.

(3) Require, by contract, that the third party implement and maintain appropriate security measures for personal information. Contracting with a

third party to maintain personal information about California residents shall not relieve the consumer credit agency of the requirements of this section.

(c) As used in this section, "significant risk" means a vulnerability score, calculated using a standard measurement system that is accepted as a best practice for the industry, to determine that the risk could reasonably result in a breach of the security of the system, as defined in subdivision (g) of Section 1798.82, of personal information, as defined in subdivision (h) of Section 1798.82.

(d) As used in this section, "compensating controls" means controls that the agency reasonably believes will prevent the computer system vulnerability as described in subdivision (a) from being exploited while the software update is being tested, assessed, and a plan for implementation is being developed, and have been adequately tested and confirmed to sufficiently offset the risk of breach caused by computer system vulnerability as described in subdivision (a).

(e) Nothing in this section shall reduce the responsibilities and obligations of a consumer credit reporting agency or third party under this title, including, but not limited to, Section 1798.81.5.

(f) The Attorney General has exclusive authority to enforce this section.

O