Date of Hearing: April 25, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 1712 (Irwin) – As Amended March 13, 2023

Proposed Consent

SUBJECT: Personal information: data breaches

SYNOPSIS

California's Data Breach Notification Law requires state and local agencies to promptly notify California residents of any agency data breaches in which their personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This author-sponsored measure proposes to add helpful information to the notification given to data breach victims under current law. First, the bill would mandate that the notification given to individuals whose social security number or driver's license or California identification card number is exposed also include the internet websites of the major credit reporting agencies. Currently, the notification need only include credit reporting agencies' toll-free telephone numbers and addresses, which is somewhat antiquated in today's world. Second, the bill would permit, but not require, notifications to include information about how to place a credit or security freeze by visiting the internet websites of the major credit reporting agencies.

Committee amendments propose to bolster these requirements in two ways. First, the required notification would also have to include the URL of the Federal Trade Commission's main website for identity theft victims, currently https://www.identitytheft.gov. Second, the notification could (but would not be required to) include the specific webpages on the major credit reporting agencies' websites where individuals can place credit or security freezes.

This bill is supported by the California Credit Union League. It has no opposition on file.

SUMMARY: Adds information regarding the internet websites of the major credit reporting agencies to the notice required to be given, under the Data Breach Notification Law, to individuals whose social security number or driver's license or California identification card number is exposed in a data breach at a state or local government agency. Permits these agencies to also inform these individuals about how to place a credit or security freeze by visiting the credit reporting agencies' websites. Specifically, **this bill**:

1) Requires the security breach notification, given to individuals whose social security number or driver's license or California identification card number is exposed in a data breach at a state or local government agency, to include the internet websites of the major credit reporting agencies.

2) Permits the security breach notification to include information about how to place a credit or security freeze by visiting the internet websites of the major credit reporting agencies.

EXISTING LAW:

1) Provides, under 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 Data Breach Notification Law. (Civ. Code §§ 1798.29, 1798.82.)

3) Defines "personal information," for purposes of the Data Breach Notification Law, to include either of the following:

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

    b) The individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: social security number; driver's license number or California identification card number; 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; medical information; health insurance information; unique biometric data generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual; or information or data collected through the use or operation of an automated license plate recognition system. (Civ. Code § 1798.29(g).)

4) Excludes from the definition of "personal information" publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code § 1798.29(h).)

5) Defines "agency," for purposes of the Data Breach Notification Law, to mean every local agency and every state office, officer, department, division, bureau, board, commission, or other state agency, but to exclude:

    a) The California Legislature.

    b) The State Compensation Insurance Fund (SCIF), except as to records containing SCIF employees' personal information. (Civ. Code § 1798.3; Civ. Code § 1798.29(k); Gov. Code § 7920.510; Cal. Const. art. VI.)

6) Requires any agency that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system, as defined, to any California resident whose unencrypted personal information, or encrypted personal information along with an encryption key or security credential, was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code § 1798.29(a).)

7) Requires the disclosure under 6) to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (*Ibid*.)

8) Requires any agency that maintains computerized data that includes personal information that the agency, person, or business does not own to, immediately following discovery of the breach, notify the owner or licensee of the information of any security breach if the personal

information was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code § 1798.29(b).)

9) Establishes comprehensive requirements for the contents of the security breach notification that an agency must give an individual in the event of a data breach. (Civ. Code § 1798.29(d).)

10) Requires the notification to include the name of the agency where the breach occurred, and pertinent information under the headings, "What Happened, "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." (Civ. Code § 1798.29(d)(1).)

11) Requires the notification to also include 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. (Civ. Code § 1798.29(d)(2)(F).)

12) Permits, but does not require, the notification to include advice on steps that people whose information has been breached may take to protect themselves. (Civ. Code § 1798.29(d)(3)(B).)

13) Defines, under federal law, a "security freeze" as a prohibition on a credit reporting agency disclosing the contents of a credit report to any person that requests it. (15 U.S.C. § 1681c-1(i).)

14) Provides, under federal law, a consumer with the right to impose a security freeze free of charge until the consumer requests otherwise. (*Ibid.*)

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

COMMENTS:

1) **Background.** California's Data Breach Notification Law requires a state or local agency to notify a California resident of any data breaches where that person's personal information was, or is reasonably believed to have been, acquired by an unauthorized person. "Personal information" means information, such as a username and password, that would allow access to one or more online accounts, as well as information, such as a social security number or credit card number, that would facilitate identity theft or financial fraud.

Data breaches are increasingly prevalent in both the private and public sectors. In February 2022, approximately 260,000 attorney discipline records from the State Bar of California appeared on a public website. (State Bar of California, *Data Breach Updates, available at* https://www.calbar.ca.gov/About-Us/News/Data-Breach-Updates.) In October 2022, Los Angeles Unified School District confirmed that approximately 2,000 student psychological evaluations (including both current and former students, some who are now adults) was exposed on the so-called "dark web" by ransomware hackers. (Keierleber, *Trove of L.A. Students' Mental Health Records Posted to Dark Web After Cyber Hack*, The74 (Feb. 22, 2023), *available at* https://www.the74million.org/article/trove-of-l-a-students-mental-health-records-posted-to-dark-web-after-cyber-hack/.) Dozens more examples can be found on the data breach disclosure website that the Office of the Attorney General maintains at

https://www.oag.ca.gov/privacy/databreach/list, as required under Civil Code § 1798.29(e) (for public entity breaches) and § 1798.82(f) (for business breaches).

Data breaches, of course, can lead to identity theft. If hackers have access to personal information such a person's name, date of birth, social security number, and drivers' license number, they may be able to open fraudulent credit card accounts, turn on utility services, and perpetrate other financial frauds by impersonating the victim.

However, remedies exist. If a potential victim is promptly notified of a data breach, one of the most effective steps they can take against identity theft is to place a security freeze on their credit report, commonly known as a "credit freeze." Almost any attempt to open a financial account is accompanied by a review of data from a credit reporting agency in order to verify a person's identity and creditworthiness. Under federal law, a person can place a credit freeze by requesting credit reporting agencies not to disclose the contents of their credit reports until further notice. (15 U.S.C. § 1681c-1(i).) The credit freeze continues until the person requests the credit reporting agency to lift it. By preventing lenders, utility companies, and so forth from being able to obtain a person's credit reports, a credit freeze prevents the opening of fraudulent accounts under their identities.

This bill would help provide information to data breach victims on how to place a credit or security freeze, and thereby better protect themselves from identity theft.

2) **Author's statement.** According to the author:

> A credit freeze or security freeze is one of the most effective defensive actions that can be taken after a data breach. By notifying credit reporting agencies that a freeze should be placed on your credit report, new requests are prevented from being processed and subsequently fraudulent new lines of credit are avoided. Californians who are victims of a data breach at a public agency should have better access to knowledge about this important step they can take to defend themselves. AB 1712 will make it more likely that notifications include this key information.

3) **The Data Breach Notification Law and AB 2301**. While no general federal data breach notification laws exist, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information. (National Conference on State Legislatures, *Security Breach Notification Laws* (Jan .17, 2022), *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.)

SB 1936 (Peace, Chap. 915, Stats. 2002) enacted the Data Breach Notification Law in California. The Data Breach Notification Law requires a state agency, or a person or business that conducts business in California, to disclose any breach of the security of data to California residents whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as a result of the breach.

Since the passage of SB 1936, the frequency and variety of data breaches has continued to increase dramatically as computing power and the public's reliance on digital information technology grow. In the United States alone, the number of reported data breaches has grown from 447 in 2012 to 1,802 in 2022, with the number of exposed records increasing 916%, from

17.3 million in 2012 to 422.14 million in 2022. (Petrosyan, *Cyber crime: number of compromises and impacted individuals in U.S. 2005-2022*, Statista (Apr. 1, 2023), *available at* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.) While these increases could result in part from increased reporting as data breach notification laws are adopted across the country, it is undeniable that the quantity and sensitivity of personal information transmitted and stored digitally has vastly increased, as has the risk of harmful data breaches.

Accordingly, California has added numerous provisions to the Data Breach Notification Law in order to protect residents as data breaches become more commonplace. For example, SB 29 (Simitian, Chap. 197, Stats. 2011) first set out statutory requirements for the contents of data breach notifications, including the provisions amended by this bill. In recent years, AB 2828 (Chau, Chap. 337, Stats. 2016) required notification of breaches of encrypted personal information if an encryption key or security credential that could render the information readable was also compromised in the breach, and AB 1130 (Levine, Chap. 750, Stats. 2019) added government-issued identification numbers and unique biometric data to the definition of "personal information."

4) **What this bill would do.** The Data Breach Notification Law specifies in some detail the content of the security notification that an agency must give a person whose personal information is subject to a data breach. Among the information that must be given is "[t]he 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." (Civ. Code § 1789.29(d)(2)(F).) This bill would amend this provision to require that agencies also provide victims with the internet websites of the major credit reporting agencies.

The Data Breach Notification Law does not require, but does permit, agencies to include in the notification "advice on steps that people whose information has been breached may take to protect themselves." (Civ. Code § 1789.29(d)(3)(B).) This bill would make this provision more specific by clarifying that this advice could include informing victims as to how to place a credit or security freeze by visiting the internet websites of the major credit reporting agencies.

Given the increasing frequency of data breaches, this bill offers a straightforward way to improve victims' chances of avoiding the time, expense, and stress of identity theft.

5) **Committee amendments—providing additional helpful information to data breach victims.** Proposed amendments would strengthen this bill's requirements in two ways. One amendment would add the Federal Trade Commission's main website for identity theft victims to the information that must be provided to data breach victims:

> **Civil Code 1798.29.** […]
>
> (d) […] (2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information: […]
>
> ***(G) The Uniform Resource Locator (URL) for the main internet website operated by the Federal Trade Commission to provide information for victims and potential victims of identity theft, which at the time the act adding this subparagraph is enacted is at https://www.identitytheft.gov.***

As described on the website, "IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process." The website includes specific steps to be taken based on the information that may have been stolen, such as a social security number, driver's license information, or bank account information.

The second amendment would clarify that agencies could include, in the information they are permitted (but not required) to provide data breach victims, URLs for the specific webpages on the major credit reporting agencies' websites where one may place credit or security freezes:

> **Civil Code 1798.29.** […]
>
> (d) […] (3) At the discretion of the agency, the security breach notification may also include any of the following: […]
>
> (B) Advice on steps that people whose information has been breached may take to protect themselves, including how to place a credit or security freeze by visiting the ~~internet website~~ ***URLs of specific pages on the internet websites*** of the major credit reporting agencies ***where an individual may place a credit or security freeze.***

Providing this specific information may enhance the speed with which data breach victims freeze their credit reports, and also help them avoid fake websites if they were to use a search engine to try to find these pages.

ARGUMENTS IN SUPPORT: California Credit Union League explains how this bill could help victims of data breaches:

> With increased cases of data breaches and identity theft, it is more important now than ever to provide clear guidance to victims on what steps to take following a data breach of their personal information. Placing a credit freeze is an effective and important step for victims to take to prevent identity theft and fraud. By requiring agencies to include the credit reporting agencies websites in the security breach notification and authorizing the notification to include steps on how to freeze your credit, AB 1712 will allow California consumers to better protect themselves and their personal information.

REGISTERED SUPPORT / OPPOSITION:

Support

California Credit Union League

Opposition

None on file

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200