Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1035 (Mayes) – As Amended April 22, 2019

SUBJECT: Personal information: data breaches

SUMMARY: This bill would require a person, business, or agency that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the system within 45 days, as specified, and would further define "reasonable security procedures and practices" for the purposes of California's Data Breach Notification Laws (DBNL). Specifically, **this bill would**:

1) Require that a person, business, or agency in California provide the required notice under the DBNL in no case more than 45 days following discovery or notification of the breach, as specified.

2) Provide, for the purposes of the DBNL and the limited private right of action in the California Consumer Privacy Act of 2018 (CCPA), that "reasonable security procedures and practices" include, but are not limited to, a cybersecurity program that reasonably conforms to the current version, or a version that has been revised within the one-year period before the date of a security breach, of any of the following:

   - The Framework for Improving Critical Infrastructure Cyber Security developed by the National Institute of Standards and Technology (NIST).

   - NIST Special Publication 800-171.

3) Make other technical and non-substantive changes.

EXISTING LAW:

1) Requires, pursuant to the DBNL, that a business that owns, licenses, or maintains PI about a California resident 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. (Civ. Code Sec. 1798.81.5.)

2) Requires, pursuant to the DBNL, that a person, business, or agency in California that owns or licenses computerized data that includes personal information to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person by a breach of the security of the system or data. The notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs. 1798.29(a), (c); 1798.82(a), (c).)

3) Requires a person or business that is the source of a breach of social security numbers or driver's license numbers, and is required to provide notice of the breach, to offer appropriate

identity theft protection or mitigation services to affected individuals at no cost, for no less than 12 months, as specified. (Civ. Code Secs. 1798.82(d)(2)(G).)

4) Requires a person or business that maintains computerized data that includes personal information that the 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 Secs. 1798.29(b); 1798.82(b).)

5) Requires the breach notification to include certain information including in part, certain titles and headings, contact information for the breached entity, the type of personal information breached, a general description of the breach incident, and the toll-free telephone numbers and addresses of the major credit reporting agencies. Also provides a model form that is deemed to comply with the requirement. (Civ. Code Secs. 1798.29(d)(1)-(2); 1798.82(d)(1)-(2).)

6) Allows at the discretion of the breached entity, the breach notification to include other information including a description of efforts to protect the information that has been breached, and advice on steps that the person whose information has been breached may take to protect himself or herself. (Civ. Code Secs. 1798.29(d)(3); 1798.82 (d)(3).)

7) Defines "PI," for purposes of the DBNL, to include 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; or health insurance information. "PI" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Secs. 1798.29(g)-(h); 1798.82(h)-(i).)

8) Authorizes, pursuant to the CCPA, any consumer whose nonencrypted or nonredacted PI, as defined, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information to institute a civil action. (Civ. Code Sec. 1798.150.)

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: This bill seeks to ensure greater protection for the PI of California residents by strengthening provisions within the DBNL and related statutes. This bill is author-sponsored.

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

> In the absence of a uniform federal law, current California law since 2003 has required data breach disclosures to be "made in the most expedient time possible and without unreasonable delay," while also working with law enforcement needs. Companies have

taken this statute to mean a variety of things. For example, in late September of 2018, Facebook reported within 72 hours that hackers could have accessed the data from tens of millions of accounts, despite the company not yet knowing the full extent of the breach. They immediately logged out up to 90 million users from their accounts and required them to reenter their information. Conversely, Google learned of a data breach that affected half a million accounts in March of 2018, but did not disclose the breach until October of 2018.

AB 1035 would require a person or business that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system within [45 days] following the discovery or notification of the breach, subject to the legitimate needs of law enforcement.

3) **California's data breach notification law (DBNL)**: Effective 2003, California became the first state in the nation to require businesses and government agencies to notify residents of security breaches if PI was, or was reasonably believed to have been, stolen. (SB 1386 (Peace, Ch. 915, Stats. 2002).)

Until January 1, 2017, the DBNL did not apply to "encrypted" information, which created an incentive for businesses and government agencies to encrypt personal data and thereby avoid the notice requirement. AB 2828 (Chau, Ch. 337, Stats. 2016) required agencies, persons, and businesses to also disclose a breach of a security of a system containing *encrypted* PI when the encryption key or security credential that could render that PI readable or useable was also compromised in the breach. Despite this change, it is important to note that notice is not required unless the data breach involved "PI" relating to a California resident. "PI" means a person's first name or first initial and last name in combination with one or more of the following data elements:

- 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;
- medical information; health insurance information; or,
- a user name or email address in combination with a password or security question and answer that would permit access to an online account.

"PI" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The DBNL has two distinct parts: one part that applies to state and local agencies, and one part that applies to private persons and businesses. In addition, California has very specific guidelines on breach notification, and the notification must include, at a minimum, the following: (1) the name and contact information of the reporting person or business; (2) a list of the types of PI that were or are reasonably believed to have been the subject of a breach; (3) whether notification was delayed as a result of law enforcement investigation; (4) a description of the breach incident; (5) toll-free phone numbers and addresses of the major

credit reporting agencies, if the breach exposed a social security number, driver's license or California identification card number; and, (6) if the person or business making the notification was the source of the breach, then it must offer to provide identity theft prevention services at no cost for at least 12 months.

4) **Requires data breach notifications to be made within 45 days**: Existing law requires that individuals are notified of a breach "in the most expedient time possible and without unreasonable delay." (*See* Civ. Code Secs. 1798.29(a) and 1798.82(a).) This bill would instead require the disclosure be provided to affected persons in the most expedient time possible and without unreasonable delay, but in no case more than 45 days following a data breach. According to the Attorney General's (AG) most recent data breach report, the average time from discovery of a breach to notification of those affected was 40 days, and the median was 30 days. In 25% of the breaches consumers were notified in 16 days or less, and in 75% of them notification was made in 50 days or less. (California Department of Justice, *California Data Breach Report*, (Feb. 2016) <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf >[as of Apr. 21, 2019].)

   Despite the average times reported by the AG above, many companies take much longer to notify individuals that their information may have been stolen, thus denying those affected the opportunity to proactively begin mitigating the risks of identity theft and fraud. For example, when the PI of at least 30,000 Kaiser employees was negligently released in 2011, Kaiser waited nearly six months before notifying affected individuals. According to the AG, this constituted unreasonable delay. (*See* Breaux et al, *California AG Cracks Down on Timing of Data Breach Disclosures*, Haynesboone, (Feb. 5, 2014).) To ensure that affected persons learn that their PI has been compromised in a timely manner, this bill would require that data breach disclosures are made in the most expedient time possible and without unreasonable delay, but in no case more than 45 days from the discovery of the breach. By This language will also ensure that if disclosure can be made earlier, the business or agency would be required to make the disclosure "in the most expedient time possible." Taking note of the average timeframes referenced by the AG above, the vast majority of breach notifications are already happening within this timeframe. Accordingly, this requirement should not be overly burdensome on business, but would ensure that disclosures are made in a reasonable amount of time so that individuals whose PI has been compromised can take appropriate steps to protect themselves from identity theft and fraud.

5) **"Reasonable security features" required by DBNL and CCPA**: On June 28, 2018, the California Legislature unanimously passed, and the Governor signed AB 375 (Chau, Ch. 55, Stats. 2018), a significant expansion of data privacy protections for Californians. That new law, the California Consumer Privacy Act (CCPA), guarantees consumers certain rights and protections with respect to the collection and sale of their PI. These rights and protections include the following:

   - The right of a consumer to access their PI. (Civ. Code Sec. 1798.100.)
   - The right to know what PI is collected about a consumer by a business. (Civ. Code Sec. 1798.110.)
   - The right to know whether PI is sold or disclosed by a business. (Civ. Code Sec. 1798.115.)

- The right to delete the PI that a business collected from a consumer. (Civ. Code Sec. 1798.105.)

- The right to opt out of the sale of PI, or opt in, in the case of minors. (Civ. Code Sec. 1798.120.)

- The right to equal service and price in goods and services, despite a consumer exercising any of the rights listed above. (Civ. Code Sec. 1798.125.)

As enacted by AB 375, the CCPA represents a legislative effort to reach an agreement on issues relating to the collection and sale of consumers' PI by businesses, both online and otherwise. Those same issues were also the subject of initiative measure, which would have been placed on the November 2018 ballot for Californian voters' consideration in the absence of a legislative solution by June 28, 2018—the deadline to remove an initiative from the November ballot. Immediately after the passage of the CCPA, the original authors of AB 375 sought to correct numerous drafting errors, make non-controversial clarifying amendments, and address several policy suggestions made by the Attorney General in a preliminary clean-up bill at the end of the 2017-2018 legislative session, SB 1121 (Dodd, Ch. 735, Stats. 2018). That bill was signed by Governor Brown on September 23, 2018.

Of particular relevance to this bill, SB 1121 specifically ensured that a private right of action in that bill applied only to the CCPA's section on data breach and not to any other section of the CCPA, as specified. (*See* Civ. Code Sec. 1798.150.) California's DBNL and the limited private right of action for data breaches under the CCPA, both require businesses to "maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the information from unauthorized access, destruction, use, modification, or disclosure. (*See* Civ. Code Secs. 1798.81.5 and 1798.150.) By pointing to cybersecurity guidelines developed by the NIST, this bill seeks to provide clarity for businesses and promote high quality cybersecurity standards. Specifically, this bill would provide that reasonable security procedures and practices include, but are not limited to a cybersecurity program that reasonably conforms to the current version, or a version that has been revised within the one-year period before the date of a security breach, of: (1) the Framework for Improving Critical Infrastructure Cybersecurity (Framework) by NIST; or, (2) NIST Special Publication 800-171.

NIST Special Publication 800-171 "provides federal agencies with a set of recommended security requirements for protecting the confidentiality of [controlled unclassified information] CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry." (Ross et al, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* NIST (Dec. 2016).) In relevant part, this bill as currently in print amends part of the DBNL and CCPA applying to the private sector, and not the provisions applying to government agencies. Accordingly, the NIST Framework, discussed more below, is arguably more appropriate as guidance for businesses than the special publication, which addresses federal agencies.

NIST first published a Cybersecurity Framework in February of 2014, and released an updated version last April. (*See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018) <https:// www.nist.gov/cyberframework/framework> [as of Apr. 21, 2019].) The Framework specifically includes guidance on passwords and other authentication methods, automated indicator sharing (to detect, mitigate, and possibly even prevent cyber attacks), and conformity assessment. NIST notes that while the Framework was developed improve cybersecurity risk management in critical infrastructure, it can be used by organizations in any sector or community. NIST further provides:

> The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.
>
> To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders. (NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, (Apr. 16, 2018), pp. 2-3.)

The NIST Framework clearly contains a wealth of helpful information for businesses seeking to create or enhance a cybersecurity system and is intended to be used to "complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program." (*Id*. at pp. 13.)

That is not to say, however, that "reasonably conforming" to the guidance provided by the Framework will necessarily result in "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," as required by the DBNL and CCPA. By NIST's own admission, the Framework creates flexible guidance for businesses to use as needed by their particular operation and existing sophistication, and is not a "one-size-fits-all" option. Arguably, incorporating this type of guidance into our current laws as a safe harbor for what constitutes reasonable security procedures and practices could ultimately be confusing from a compliance, and potentially

litigation, standpoint. As such, if this Committee were to approve this bill, it may wish to remove the references to the NIST Framework and special publication 800-171.

Suggested amendment:

On page 10, strike lines 32-40.

On page 18 and 19, strike lines 39-40 and 1-7, respectively.

Related legislation: AB 1130 (Levine, 2019) would add government-issued identification numbers and biometric data, as defined, to the definition of personal information in the DBNL. This bill is currently in the Assembly Appropriations Committee.

6) **Prior legislation**: AB 2828 (Chau, Ch. 337, Stats. 2016) required agencies, persons, and businesses to disclose the breach of the security of a system containing encrypted personal information when the encryption key or security credential that could render that personal information readable or useable is also compromised in the breach.

SB 570 (Jackson, Ch. 543, Stats. 2015) required, in the event of a data breach, agencies and persons conducting business in California to provide affected individuals with a notice entitled "Notice of Data Breach," in which required content is presented under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

AB 1710 (Dickinson, Ch. 855, Stats. 2014) enacted various changes to the DBNL including requiring the source of the breach to offer appropriate identity theft prevention and mitigation services to consumers at no cost.

SB 46 (Corbett, Ch. 396, Stats. 2013) revised certain data elements included within the definition of personal information under the DBNL, by adding certain information that would permit access to an online account and imposed additional requirements on the disclosure of a breach of the security of the system or data in situations where the breach involves personal information that would permit access to an online or email account.

SB 24 (Simitian, Ch. 197, Stats. 2011) required any agency, person, or business that is required to issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, and required any agency, person, or business that is required to issue a security breach notification to more than 500 California residents to electronically submit a single sample copy of that security breach notification to the Attorney General.

AB 1950 (Wiggins, Ch. 877, Stats. 2004) required a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure. AB 1950 also required a business that discloses personal information to a nonaffiliated third party, to require by contract that those entities maintain reasonable security procedures.

SB 1386 (Peace, Ch. 915, Stats. 2002) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rapier / P. & C.P. / (916) 319-2200