Date of Hearing: March 17, 2015

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Gatto, Chair
AB 259 (Dababneh) – As Introduced February 9, 2015

SUBJECT: Personal information: privacy

SUMMARY: Requires a public agency that is the source of a data breach to offer at least 12 months of identity theft prevention and mitigation services at no cost to affected consumers. Specifically, **this bill**:

1) Requires a public agency that is the source of a data breach and is required to provide affected persons with notice of the breach to provide at least 12 months of appropriate identity theft prevention and mitigation services at no cost to the affected persons.

2) Requires a public agency to give affected persons all information necessary to take advantage of the offer for identity theft prevention and mitigation services.

3) Requires a public agency to offer identity theft prevention and mitigation services only if the breach exposed, or may have exposed, a person's name in combination with a Social Security number or a driver's license number.

4) Requires a public agency that delays the specified notification at the direction of law enforcement to make the notification promptly after a law enforcement agency determines that notification will not compromise any criminal investigation.

5) Makes other technical and nonsubstantive amendments.

EXISTING LAW:

1) Requires a public agency, person, or business 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. 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. Note that this requirement does not apply to the Judiciary, the Legislature, or the University of California. (Civil Code (Civ. Code) Sections 1798.29(a), (c); 1798.82(a), (c))

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

3) Requires a public agency, person, or business that maintains computerized data that includes personal information that the agency, 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 1798.29(b), 1798.82(b))

4) Defines "personal information," for purposes of the breach notification statute, 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. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code 1798.29(g), (h), 1798.82(h), (i))

FISCAL EFFECT: Unknown

COMMENTS:

1) Purpose of this bill. This bill is intended to provide individuals affected by a state or local agency data breach with at least 12 months of identity theft protection for free. While existing law already requires any private business responsible for a significant breach to offer at least 12 months of identity theft prevention mitigation services, no such requirement exists for public agencies. AB 259 would extend these protections to include state and local agencies. This measure is author-sponsored.

2) Author's statement. According to the author's office, "Whether a data breach occurs at a state agency or a business, the same standards should be in place to protect consumers A breach resulting in the release of Social Security or driver license numbers can lead to identity theft, forcing consumers to monitor their personal information for years to come."

3) Recent data breaches. More than 80 million people in the United States were impacted by the February 2015 data breach at health insurer Anthem. Information stolen in the breach included current and former customers' names, birth dates, medical identification numbers, Social Security numbers, home addresses, email addresses, and employment and income data.

   In fact, the Anthem breach was just the latest in a string of high profile data breaches; 2014 was a record-setting year in terms of the number of security breaches reported. According to a January 2015 report by the California Attorney General's Office, 187 breaches were reported to the California Department of Justice in 2014, compared to 167 in 2013 and 131 in 2012. According to a national database of breaches maintained by the Privacy Rights Clearinghouse, more than 815 million records have been compromised in more than 4,489 publicly acknowledged data breaches since 2005.

   Unfortunately, state and local agencies are not immune to data breaches. During 2012-2014, the following California public agencies reported breaches: California State University, Department of Corrections and Rehabilitation, Department of Public Health, Department of State Hospitals, Correctional Health Care Services, Department of Social Services, Department of Justice, Department of Child Support Services, Employment Development Department, and the Department of Motor Vehicles.

4) California's Data Breach Notification Law. In 2003, California became the first state in the nation to require businesses and government agencies to notify California residents of

security breaches if unencrypted personal information was, or was reasonably believed to have been, stolen. (SB 1936 (Peace), Chapter 915, Statutes of 2002)

The notification law does not apply to "encrypted" information, which creates an incentive for businesses and government agencies to encrypt personal data and thereby avoid the notice requirement. Also, notice is not required unless the data breach involved "personal information" relating to a California resident. "Personal information" means a person's first name or first initial and last name in combination with one or more of the following data elements:

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;
d) Medical information; health insurance information; or
e) A user name or email address in combination with a password or security question and answer that would permit access to an online account.

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

The Data Breach Notification Law has two distinct parts: one part that applies to state and local agencies, which is located in the Information Practices Act of 1977 (Civ Code 1798.29), and one part that applies to businesses (Civ. Code 1798.82). Both parts began as mirror images of each other. Over the years, however, as the Legislature has refined and updated the Data Breach Notification Law, the language of the two parts has not always been kept consistent.

Most recently, the Legislature passed and the Governor signed AB 1710 (Dickinson), which required an affected business to offer appropriate identity theft prevention and mitigation services for at least 12 months at no cost to people affected by the breach, in cases where a breach involved Social Security or driver's license numbers. AB 259 would extend these same protections to persons affected by a state or local agency data breach.

5) <u>The benefits of identity theft prevention and mitigation services</u>. According to the author, the term "identity theft prevention and mitigation services" includes credit report monitoring services, which help prevent fraud and identity theft by giving consumers ongoing information about credit card account balance increases and new loans and credit cards opened in the consumer's name. Identity theft prevention and mitigation services may also include security freeze services offered by credit reporting agencies, which stop identity thieves from opening up new accounts in a victim's name by "freezing" the victim's credit report, so that lending institutions cannot check a credit report or credit score to approve new loans or credit cards.

6) <u>Questions about the "if any," clause</u>. There has been some discussion within the legal community as to whether or not the phrasing of the existing statute as it applies to businesses – which is mirrored in this bill for public agencies – is open to more than one interpretation. As passed by the Legislature and signed by the Governor, AB 1710 (Dickinson), requires a business that issues a breach notification to offer "appropriate identity theft prevention and

mitigation services, if any" to affected individuals at no cost. However, the question has been raised as to whether or not the offer of services itself is required or discretionary.

Read plainly, the "if any" clause (Civ Code 1798.29 (d)(2)(G)) would presumably modify the preceding phrase "appropriate identity theft prevention and mitigation services" – i.e., if there are no prevention or mitigation services that are appropriate for a consumer after a particular breach, then the business is not required to offer services. For example, a retail breach involving the theft of credit card numbers might be appropriately mitigated by re-issuing cards with new card numbers rather than setting up credit reporting monitoring services for a year, since theft of a credit card number is not enough information for criminals to open up new accounts in the cardholder's name. However, the presumption is in favor of the provision of services unless it is obvious that no service is appropriate.

Conversely, the law firm Morrison & Foerster suggested in an online Client Alert on October 9, 2014, that the "if any" clause could be interpreted to modify the "offer" of services itself to make it voluntary. Under this reading, a business would simply be permitted by statute – not required – to offer identity theft prevention and mitigation services after a breach.

The question is pertinent to this bill because AB 259's language mirrors the existing language in question from AB 1710 in applying the requirement to public agencies. While perhaps it would be ideal to clarify the matter in statute, the author's office has stated to Committee staff that it is the intent of this bill to require – not simply authorize – public agencies to provide affected consumers with identity theft prevention and mitigation services for a minimum of 12 months.

The author's stated intent would appear to be in line with the intent of AB 1710 (Dickinson) as well. The June 24, 2014, Senate Judiciary Committee analysis of AB 1710 (Dickinson) describes that bill as imposing a requirement, not a discretionary authorization: "This bill would also require the person or business providing notification that was the source of the breach to provide to affected consumers with identity theft prevention and mitigation services for a minimum of 12 months."

As such, it is the understanding of Committee staff that the language of this bill requires an offer of identity theft prevention and mitigation services, except in those cases where no such service would be appropriate.

7) Arguments in support. According to the California School Employees Association: "Once you are a victim of identity theft, it is very difficult to resolve these issues and quite costly and time consuming. AB 259 is an important step in helping the victims of identity theft to repair their credit and get their financial lives back in order."

8) Related legislation. SB 34 (Hill) amends the Data Breach Notification Law to add to the definition of "personal information" any information or data collected through the use or operation of an automated license plate recognition system. SB 34 is currently pending in the Senate Transportation and Housing Committee.

9) Prior Legislation. AB 1710 (Dickinson and Wieckowski), Chapter 855, Statutes of 2014, required a person or business that is the source of a breach of Social Security numbers or driver's license numbers to offer an identity theft protection or mitigation service to affected

individuals at no cost, for no less than 12 months. It expands the information security law to require businesses that maintain, own or license the personal information of California residents to use reasonable and appropriate security measures to protect the information. It also prohibits the sale or marketing of Social Security numbers, with certain exceptions.

SB 46 (Corbett), Chapter 396, Statutes of 2013, revised certain data elements included within the definition of personal information under California's Data Breach Notification Law, 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), Chapter 197, Statutes of 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 1298 (Jones), Chapter 699, Statutes of 2007, among other things, added medical information and health insurance information to the data elements that, when combined with the individual's name, would constitute personal information requiring disclosure when acquired, or believed to be acquired, by an unauthorized person due to a security breach.

AB 1950 (Wiggins),Chapter 877, Statutes of 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 1936 (Peace), Chapter 915, Statutes of 2002, enacted California's Data Breach Notification Law and required a public agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information to disclose any breach of the security of the data to California's residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. SB 1936 permitted notifications to be delayed if a law enforcement agency determines that it would impede a criminal investigation, and required an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data.

REGISTERED SUPPORT / OPPOSITION:

Support

Association of California Life and Health Insurance Companies
California Bankers Association
California Business Properties Association
California Chamber of Commerce

California Credit Union League
California Grocers Association
California Land Title Association
California Retailers Association
California School Employees Association
Direct Marketing Association
Retail Industry Leaders Association

Opposition

No opposition on file.

Analysis Prepared by: Jennie Bretschneider/P. & C.P./(916) 319-2200