STATE OF CALIFORNIA
Franchise Tax Board

Analysis of Amended Bill

Author: Levine	Sponsor:	Bill Number: AB 1130
Analyst: Elaine Warneke	Phone: (916) 845-7746	Introduced: February 21, 2019 Amended: May 16, 2019
Attorney: Shane Hofeling	Related Bills: See Legislative History	

Subject: Updated Definition of Personal Information

Summary

This bill would, under the Civil Code, change the definition of personal information to include certain government identification numbers (IDs) and biometric data.

Recommendation – No position.

Summary of Amendments

This bill, as introduced on February 21, 2019, would include government-issued IDs and biometric data in the definition of "personal information" in the California Data Breach Notification Law (DBNL) as it applies to both public agencies and businesses; and would make other nonsubstantive technical changes.

The May 16, 2019, amendments replaced government-issued IDs with tax IDs, passport numbers, military IDs, and unique IDs issued on a government document, added a breach involving biometric data to the current security breach notification process, and made other nonsubstantive technical changes.

This is the department's first analysis of the bill and only addresses the provisions that impact the department.

Reason for the Bill

The reason for the bill is to expand the definition of personal information that must be treated as confidential information under California's DBNL.

Effective/Operative Date

This bill would become effective and operative January 1, 2020.

Federal/State Law

Current federal and state law provides that income tax returns and tax information are confidential and may not be disclosed, unless specifically authorized by statute. Improper disclosure of federal tax information is punishable as a felony, and improper disclosure of state tax information is punishable as a misdemeanor.

The Information Practices Act of 1977 (Act) requires an agency, as defined, to notify a resident of California in the event their personal information has been acquired by an unauthorized person due to a breach of security of that agency's computer system. A "breach of the security of the system" is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information; however, an employee or agent of an agency is authorized to acquire personal information to perform his or her work duties.

For purposes of the Act, "agency" means every state office, officer, department, division, bureau, board, commission, or other state agency, except for the California Legislature, any agency established under Article VI of the California Constitution, the State Compensation Insurance Fund, as specified, and a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

"Personal information" is defined as either of the following:

A. An 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 card number, or debit card number along with the required security code, access code, or password that would permit access to an individual's financial account.
    - Medical information.
    - Health insurance information.
    - Information or data collected through the use or operation of an automated license plate recognition system, as defined in Civil Code section 1798.90.5; or

B. 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 legally made available to the general public from federal, state, or local government records.

The security breach notification is to be written in plain language in the format specified and must include the following information:

- The name and contact information of the reporting agency.
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- The date, estimated date, or date range the breach occurred, if known.
- Whether the notification was delayed as a result of a law enforcement investigation, if known.
- A general description of the breach, if that information is possible to determine at the time of notice.
- The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number, or a drivers' license or California identification number.

Current law requires the inclusion of an electronic or written notice titled "Notice of Data Breach" (Notice) with a security breach notification letter. The content for the Notice must be presented under the following headings:

- "What Happened"
- "What Information Was Involved"
- "What We Are Doing"
- "What You Can Do"
- "Other Important Information"
- "For More Information"

Additional information may be provided as a supplement to the Notice. The format of the Notice must be designed to call attention to the nature and significance of the information it contains. The title and headings in the Notice must be clearly and conspicuously displayed and the text of the Notice and any other notice provided must be no smaller than 10-point font type.

Existing law requires conspicuous posting with a minimum posting period of 30 days of the Notice.

When a single breach results in security breach notifications, as required pursuant to the California DBNL, that must be issued to more than 500 California residents, then the agency, person, or business is required to electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the California Attorney General.

The department's current disclosure policies and procedures already encompass and protect any taxpayer or employee confidential information, including the IDs specified in this bill. The department does not collect taxpayer biometric data, however the department does fingerprint employees during its hiring process, but does not maintain the fingerprints in a database.

This Bill

This bill would expand the definition of "personal information" for purposes of the DBNL, as it applies to both public agencies and businesses, to include tax IDs, passport numbers, military IDs, and unique IDs issued on a government document and unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data. It also would allow a person or business that is required to issue a security breach notification involving biometric data, to include instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

Implementation Considerations

Implementing this bill would occur during the normal annual updates, and would not significantly impact the department's programs and operations.

Legislative History

AB 1035 (Mayes, 2019/2020) 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 72 hours following discovery or notification of the breach, subject to the legitimate needs of law enforcement. AB 1035 is currently referred to the Senate Judiciary Committee.

AB 241 (Dababneh, 2017/2018) would have required 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. AB 241 failed to pass out of the Assembly Appropriations Committee.

AB 2678 (Irwin, 2017/2018) would have required the notification provided to a person affected by a breach to include, among other things, notice that the affected person may elect to place a security freeze on his or her credit report and an explanation of how a security freeze differs from identity theft prevention and mitigation services. AB 2678 bill failed to pass. From the Consent Calendar, AB 2678 was placed in the Senate inactive file.

Other States' Information

Since this bill is administrative in nature, a review of other states' income tax laws would not be relevant.

Fiscal Impact

This bill would not significantly impact the department's costs.

Economic Impact

Revenue Estimate

This bill, as amended May 16, 2019, would not impact state income or franchise tax revenue.

This analysis does not account for changes in employment, personal income, or gross state product that could result from this bill or for the net final payment method of accrual.

Legislative Staff Contact

Elaine Segarra Warneke
Legislative Analyst, FTB
(916) 845-7746
elaine.warneke@ftb.ca.gov

Jame Eiserman
Revenue Manager, FTB
(916) 845-7484
jame.eiserman@ftb.ca.gov

Jahna Carlson
Assistant Legislative Director, FTB
(916) 845-5683
jahna.carlson@ftb.ca.gov