STATE OF CALIFORNIA
Franchise Tax Board

Analysis of Amended Bill

Author: Irwin	Sponsor:	Bill Number: AB 2678
Analyst: Janet Jennings	Phone: (916) 845-3495	Amended: June 21, 2018
Attorney: Bruce Langston	Related Bills: See Legislative History	

Subject: State Agencies, Persons, or Businesses Disclose Any Breach of Security or Data / Notification Requirements

Summary

Under the Civil Code, this bill would modify the notification requirements applicable to a state agency, person, or business that owns or licenses computerized data that includes personal information, upon discovery or notification of a breach of the security of that data.

Recommendation – No position.

Summary of Amendments

The June 21, 2018, amendments expanded the modified reporting requirements applicable to security breach notifications to apply to state agencies as well as to a person or business.

This is the department's first analysis of the bill.

Reason for the Bill

The reason for the bill is to require state agencies, that own or license computerized data that includes personal information, in addition to a person or business that have discovered or been notified of a data breach, to include specified information in a required notification of a security breach.

Effective/Operative Date

This bill would be effective January 1, 2019, and would apply to specified security breach notifications issued on or after that date.

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. Any Franchise Tax Board employee or member responsible for the improper disclosure of federal or state tax information is subject to criminal prosecution or fines, or both. 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," and
- "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 type.

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

This Bill

This bill would modify reporting requirements applicable to state agencies that own or license computerized data that includes personal information, and persons or businesses upon discovery or notification of a breach in the security of specified data, to include:

(1) The Internet Web site address of each of the major credit reporting agencies.
(2) A notice instructing the affected person that information related to security freezes and fraud alerts is available from the major credit reporting agencies.

Implementation Considerations

Implementing this bill would not significantly impact the department's programs and operations.

Legislative History

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. This bill failed passage from the Assembly Appropriations Committee.

AB 608 (Irwin, 2017/2018) would prohibit consumer credit reporting agencies from charging fees in connection with placing or removing security freezes for protected consumers, defined as individuals who are under 16, incapacitated, or under a county welfare or county probation department's jurisdiction. This bill is currently in the Senate Judiciary Committee.

AB 1859 (Chau, 2017/2018) would require a consumer credit reporting agency that knows of a vulnerability that could compromise the security of personal information for which there is an update to address, to apply that update or be held liable for any resulting damages. This bill is currently in the Senate Judiciary Committee.

SB 1121 (Dodd, 2017/2018) would, in relevant part, create a more robust enforcement mechanism for violations of the Data Breach Notification law. This bill is currently in the in the Assembly Privacy and Consumer Protection Committee.

AB 964 (Chau, Chapter 522, Statutes of 2015) defined "encrypted" for Sections 1798.29 and 1798.82 of the Civil Code.

SB 570 (Jackson, Chapter 573, Statutes of 2015) modified the requirements applicable to security breach notifications.

AB 2374 (Hernández, Chapter 645, Statutes of 2012) prohibited credit reporting agencies from charging specified consumers any fee for the initial placement of a security freeze, but authorized such agencies to charge a fee of up to $5 for lifting, removing, or replacing a security freeze.

SB 24 (Simitian, Chapter 197, Statutes of 2011) added the minimum information to be provided in a security breach notification.

Other States' Information

The states surveyed include *Florida, Illinois, Massachusetts, Michigan, Minnesota,* and *New York.* These states were selected due to their similarities to California's economy, business entity types, and tax laws. Florida does not have an individual income tax. The remaining states have statutes similar to California law regarding breach of systems containing personal information. Research failed to identify any statutes specifically related to providing the information requirements of this bill.

Fiscal Impact

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

Economic Impact

This bill would not impact the state's income tax revenue.

Support/Opposition

Support: None provided.

Opposition: None provided.

Arguments

Proponents: Some may argue that this bill would require additional relevant contact information and of security freezes and alerts in notifications related to a security breach.

Opponents: Some may argue that this bill would place unnecessary additional mandates on the state's businesses and government.

Legislative Staff Contact

Janet Jennings
Legislative Analyst, FTB
(916) 845-3495
janet.jennings@ftb.ca.gov

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

Diane Deatherage
Legislative Director, FTB
(916) 845-6333
diane.deatherage@ftb.ca.gov