**Franchise Tax Board**

# ANALYSIS OF AMENDED BILL

| | | | | | |
|---|---|---|---|---|---|
| Author: | Jackson | Analyst: | Janet Jennings | Bill Number: | SB 570 |
| Related Bills: | See Legislative History | Telephone: | 845-3495 | Amended Date: | April 6, 2015 |
| | | Attorney: | Bruce Langston | Sponsor | |

| | |
|---|---|
| **SUBJECT:** | State Agencies Disclose Any Breach of Security or System or Data/Notification Requirement Specifications |

## SUMMARY

This bill, under the Civil Code, would modify the requirements applicable to security breach notifications.

This analysis only addresses the provisions of the bill that impact the department's programs and operations.

## RECOMMENDATION

No position.

### Summary of Amendments

The April 6, 2015, amendments removed legislative intent language and replaced it with the provisions discussed in this analysis. This is the department's first analysis of the bill.

## REASON FOR THE BILL

The reason for the bill is to provide an additional notice requiring specified information to be attached to security breach notification letters.

## EFFECTIVE/OPERATIVE DATE

This bill would be effective January 1, 2016, and would apply to 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 (FTB) 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.

| Board Position: | | | | | | Executive Officer | Date |
|---|---|---|---|---|---|---|---|
| | S | | NA | X | NP | | |
| | SA | | O | | NAR | Selvi Stanislaus | 5/11/15 |
| | N | | OUA | | | | |

Current state law requires a state agency (including the FTB) 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.

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

(1) A person'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;
- Medical information; and
- Health insurance information.

(2) 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 information that is legally made available to the general public from federal, state, or local government records.

State law requires notification to be made in the most expedient time possible and without unreasonable delay. If the agency maintains computerized data, but does not own the data, the agency must notify the owner or licensee of the information of the breach immediately following discovery. State law requires notification to be made by either written, electronic, or substitute notice. Any agency that maintains its own notification procedures is considered to be in compliance. Persons must be notified in accordance with those procedures and those procedures must be consistent with the timing requirements of current law.

Current state law requires a security breach notification to be written in plain language, and include the following information in the notices issued by any person, business, or state agency to a California resident:

- Name and contact information of the reporting agency, person, or business;
- List of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- When the notice was provided, date of breach, estimated date of breach, or date range and date of the notice, if determinable;
- Whether notification was delayed as a result of law enforcement investigation;

- General description of the breach incident; and
- Toll-free telephone number and addresses of major credit reporting agencies if breach exposed a social security number or a driver's license or California identification card number.

Additionally, at the discretion of the agency, person, or business issuing the security breach, notification may also include any of the following information:

- Information about what the agency has done to protect individuals whose information has been breached; and
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

Current law provides that any person, business, or agency required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system must also electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information to the Attorney General. A single sample copy of a security breach notification would be excluded from subdivision (f) of Section 6254 of the Government Code, which prohibits the disclosure of certain public records, and requires that substitute notice be provided to the Office of Information Security within the California Technology Agency,[1] in addition to media outlets.

**THIS BILL**

This bill would require the inclusion of a one page 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," and
- "For More Information".

[1] Substitute notice consists of an e-mail notice when the person or business has an e-mail address for the subject persons, conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one, and notification to major statewide media and the Office of Information Security and Privacy Protection within the California Technology Agency.

Additional information may be provided as a supplement to the Notice. The format of the one page 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.

The bill would modify conspicuous posting requirements for substitute notice to:

- Specify a minimum posting period of 30 days of the notice.
- Define "Conspicuous posting" to mean providing a link to the notice on the home page that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding line of the same size by symbols or other marks that call attention to the link.

**IMPLEMENTATION CONSIDERATIONS**

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

**LEGISLATIVE HISTORY**

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

**OTHER STATES' INFORMATION**

The laws of the states of *Florida, Illinois, Massachusetts, Michigan, Minnesota,* and *New York* were reviewed. These states were selected due to their similarities to California's economy, business entity types, and tax laws. All of these states have statutes for the breach of systems containing personal information similar to California's statutes. Notice is required for residents whose information may have been compromised. In certain circumstances, *New York* and *Minnesota* require notification to credit bureaus, or the state consumer protection agency.

**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[2]**

Support: Privacy Rights Clearinghouse.

Opposition: None on file.

---

[2] Reported in the Senate Judiciary Committee bill analysis as amended April 6, 2015.

**ARGUMENTS**

Proponents: Some may argue that this bill would require additional clarity including relevant self-help and contact information 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

Gail Hall
Legislative Director, FTB
(916) 845-6333
gail.hall@ftb.ca.gov