

ANALYSIS OF AMENDED BILL

Author: Chau Analyst: Janet Jennings Bill Number: AB 964
 See Legislative History
 Related Bills: History Telephone: 845-3495 Amended Date: March 26, April 23, May 5, and May 13, 2015
 Attorney: Bruce Langston Sponsor _____

SUBJECT:	State Agencies Notify Attorney General of Discovery Date of Breach of Security System
-----------------	---------------------------------------------------------------------------------------

SUMMARY

This bill would, under the Civil Code, require the Attorney General be notified of the date of the discovery of a specified security breach.

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

RECOMMENDATION

No position.

Summary of Amendments

The March 26, 2015, amendments removed intent language and added provisions related to security breach notification requirements. The April 23, 2015, amendments removed specific notification criteria from the bill and the May 5, 2015, amendments made a technical correction. The May 13, 2015, amendments added to the definition of “encrypted.”

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

REASON FOR THE BILL

The reason for the bill is to strengthen California’s data breach notification law.

EFFECTIVE/OPERATIVE DATE

This bill would become effective and operative January 1, 2016.

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
<input type="checkbox"/> S <input type="checkbox"/> NA <input checked="" type="checkbox"/> X <input type="checkbox"/> NP <input type="checkbox"/> SA <input type="checkbox"/> O <input type="checkbox"/> NAR <input type="checkbox"/> N <input type="checkbox"/> OUA _____	Selvi Stanislaus	5/19/15

Current state law requires a state agency, including the FTB, to notify a resident of California in the event their encrypted personal information has been acquired by an unauthorized person due to a breach of the 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.
 - 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;
- If determinable when the notice was provided, date of breach, estimated date of breach, or date range and date of the notice;
- Whether notification was delayed as a result of law enforcement investigation;
- General description of the breach incident; and

- Toll-free telephone numbers 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, any person, business, or agency that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system is required to 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

The bill would require any person, business, or agency, including the FTB that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system to inform the Attorney General of the date of the discovery of the breach.

This bill would also define "encrypted" as rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

IMPLEMENTATION CONSIDERATIONS

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

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.

LEGISLATIVE HISTORY

SB 570 (Jackson, 2015/2016) would require additional notice providing specified information to be attached to security breach notification letters. This bill passed the Senate Appropriations Committee.

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/OPPOSITION²

Support: None on file.

Opposition: America's Health Insurance Plans
California Bankers Association
California Chamber of Commerce
California Credit Union League
California Grocers Association
California Hospital Association
California Land Title Association
California Medical Association
California Retailers Association
CTIA – The Wireless Association
Direct Marketing Association
Internet Association

² As reported in the Assembly Committee on Privacy and Consumer Protection analysis of the bill as amended April 23, 2015.

ARGUMENTS

Proponents: Some may argue this bill would allow the Attorney General to ensure security breach notifications are sent timely.

Opponents: Some may argue that this bill is unnecessary as the sample notice required to be sent to the Attorney General is dated when sent and contains the date, estimated date or date range within which the breach occurred.

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