

BILL ANALYSIS

Department, Board, Or Commission	Author	Bill Number
Franchise Tax Board	Chau	AB 964

SUBJECT

State Agencies Submit Electronic Notification of Breach of Security

SUMMARY

This bill would define “encrypted” for Sections 1798.29 and 1798.82 of the Civil Code.

The bill includes language to prevent chaptering issues with SB 34 (Hill) and SB 570 (Jackson).

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.

Current state law requires a state agency, including the FTB, to notify a resident of California in the event their unencrypted 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.

Gail Hall, FTB Contact Person
(916) 845-6333 (Office)

Executive Officer
Selvi Stanislaus

Date
9/10/15

“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:

- The name and contact information of the reporting agency, person, or business;
- A 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;
- A general description of the breach incident; and
- The 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

This bill, for purposes of determining when a person, business, or, state or local agency is required to disclose a system security breach, would 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.

LEGISLATIVE HISTORY

SB 570 (Jackson, 2015/2016) would require an additional notice providing specified information to be attached to security breach notification letters. SB 570 was enrolled on September 8, 2015.

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.

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.

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.

APPOINTMENTS

None.

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, and Internet Association.

VOTES

	Date	Yes	No
Concurrence	09/08/15	63	11
Senate Floor	09/03/15	27	11
Assembly Floor	06/03/15	69	7

LEGISLATIVE STAFF CONTACT

Contact

Work

Marybel Batjer, Agency Secretary, GovOps

916-651-9024

Jennifer Osborn, Deputy Secretary, Fiscal Policy and Administration, GovOps

916-651-9100

Selvi Stanislaus, Executive Officer, FTB

916-845-4543

Gail Hall, Legislative Director, FTB

916-845-6333

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