

ANALYSIS OF ORIGINAL BILL

Franchise Tax Board

Author: Simitian Analyst: Janet Jennings Bill Number: SB 24
Related Bills: See Legislative History Telephone: 845-3495 Introduced Date: December 6, 2010
Attorney: Patrick Kusiak Sponsor: _____

SUBJECT: State Agencies Notify California Residents Of Any Breach Of Security Of System Or Data/Additional Notification Requirements/If Notification To More Than 500 Residents Must Also Submit Electronically To Attorney General

SUMMARY

This bill would define the minimum information to be provided in a security breach notification.

PURPOSE OF THE BILL

According to the author's office, the purpose of this bill is to provide clarity in security breach notification letters.

EFFECTIVE/OPERATIVE DATE

This bill would be effective January 1, 2012, and would apply to security breach notifications issued on or after that date.

POSITION

Pending.

ANALYSIS

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.

Current state law requires a state agency 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.

Board Position:

_____ S _____ NA _____ NP
_____ SA _____ O _____ NAR
_____ N _____ OUA X PENDING

Department Director

Date

Selvi Stanislaus

01/31/11

“Personal information” is defined as 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.

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.

THIS BILL

This bill would require 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.
- 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.
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

Under this bill, 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 shall 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.

This bill revises existing law to require that substitute notice be provided to the Office of Information Security within the office of the State Chief Information Officer¹, in addition to media outlets.

LEGISLATIVE HISTORY

SB 20 (Simitian, 2009/2010) would have provided the same requirements as this bill. Governor Schwarzenegger vetoed SB 20. (See Appendix B for the complete veto message.)

SB 1166 (Simitian, 2009/2010) would have provided the same requirements as this bill. Governor Schwarzenegger vetoed SB 1166. (See Appendix A for the complete veto message.)

AB 779 (Jones, 2007/2008) would have the same requirements as this bill, except it would have reduced the cost threshold under which state agencies can elect to provide substitute notice in the event of a breach of security of data systems containing personal information. Governor Schwarzenegger vetoed AB 779. (See Appendix C for the complete veto message.)

AB 1779 (Jones, 2007/2008) would have prohibited a state agency from retaining payment related data and would have required that a state agency provide the Office of Information Security and Privacy Protection with a copy of the notice sent to California residents when a breach of security of a system containing personal information has occurred. AB 1779 was held in the Senate Judiciary Committee.

SB 852 (Bowen, 2005/2006) proposed to expand notification of breaches of security requirements to include breaches of computerized data in any format. This bill failed passage out of the Assembly Business and Professions Committee.

SB 1744 (Bowen, 2005/2006) proposed to require an agency that suffers a breach of the security of a system containing personal data to provide a credit monitoring service to the affected persons for up to one year, at no charge. This bill failed passage out of the Senate Business and Professions Committee.

SB 1279 (Bowen, 2003/2004) would have applied the notice requirements for computerized data that had been breached to security breaches for all types of data. This bill failed passage out of the Assembly Business and Professions Committee.

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 State and Consumer Services Agency

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

There would be no impact to department costs to implement this bill because the bill is consistent with department practice.

ECONOMIC IMPACT

This bill would not impact state income tax revenues.

LEGISLATIVE STAFF CONTACT

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

Revenue Manager
Monica Trefz
(916) 845-4002
monica.trefz@ftb.ca.gov

Asst. Legislative Director
Patrice Gau-Johnson
(916) 845-5521
patrice.gaujohnson@ftb.ca.gov

Appendix A

BILL NUMBER: SB 1166
VETOED DATE: 09/29/2010

To the Members of the California State Senate:

I am returning Senate Bill 1166 without my signature.

This bill would require any agency, person, or business that must issue an information security breach notification pursuant to existing law to also fulfill certain additional requirements pertaining to the security breach notification.

California's landmark law on data breach notification has had many beneficial results. Informing individuals whose personal information was compromised in a breach of what their risks are and what they can do to protect themselves is an important consumer protection benefit. This bill is unnecessary, however, because there is no evidence that there is a problem with the information provided to consumers. Moreover, there is no additional consumer benefit gained by requiring the Attorney General to become a repository of breach notices when this measure does not require the Attorney General to do anything with the notices.

Since this measure would place additional unnecessary mandates on businesses without a corresponding consumer benefit, I am unable to sign this bill.

Sincerely,

Arnold Schwarzenegger

Appendix B

BILL NUMBER: SB 20
VETOED DATE: 10/11/2009

To the Members of the California State Senate:

I am returning Senate Bill 20 without my signature.

This bill would require any agency, person, or business that must issue an information security breach notification pursuant to existing law to also fulfill certain additional requirements pertaining to the security breach notification.

California's landmark law on data breach notification has had many beneficial results. Informing individuals whose personal information was compromised in a breach of what their risks are and what they can do to protect themselves is an important consumer protection benefit. This bill is unnecessary, however, because there is no evidence that there is a problem with the information provided to consumers. Moreover, there is no additional consumer benefit gained by requiring the Attorney General to become a repository of breach notices when this measure does not require the Attorney General to do anything with the notices. Since this measure would place additional unnecessary mandates on businesses without a corresponding consumer benefit, I am unable to sign this bill.

Sincerely,

Arnold Schwarzenegger

Appendix C

BILL NUMBER: AB 779
VETOED DATE: 10/13/2007

To the Members of the California State Assembly:

I am returning Assembly Bill 779 without my signature.

Protecting the personal information of every Californian is very important to me and I am committed to strong laws that safeguard every individual's privacy and prevent identity theft. Clearly, the need to protect personal information is increasingly critical as routine commercial transactions are more and more exclusively accomplished through electronic means.

However, this bill attempts to legislate in an area where the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers. In addition, the Payment Card Industry has already established minimum data security standards when storing, processing, or transmitting credit or debit cardholder information. This industry has the contractual ability to mandate the use of these standards, and is in a superior position to ensure that these standards keep up with changes in technology and the marketplace. This measure creates the potential for California law to be in conflict with private sector data security standards.

While I support many of the provisions of this bill, it fails to provide clear definition of which business or agency "owns" or "licenses" data, and when that business or agency relinquishes legal responsibility as the owner or licensee. This issue and the data security requirements found in this bill will drive up the costs of compliance, particularly for small businesses.

I encourage the author and the industry to work together on a more balanced legislative approach that addresses the concerns outlined above.

Sincerely,

Arnold Schwarzenegger