

BILL ANALYSIS

Analyst: Deborah Barrett
Work Phone: 845-4301

Department, Board, Or Commission	Author	Bill Number
Franchise Tax Board	Simitian	SB 20

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 do the following:

- Require state agencies to provide specific information when notifying California residents of a breach of security of a system containing personal information,
- Require state agencies to provide a security breach notification electronically to the Attorney General when a single breach involves more than 500 California residents, and
- Require state agencies to provide the Office of Information Security within the Office of the Chief Information Officer with a security breach notification when substitute notice is used.

This bill would also place requirements on entities other than state agencies that do not impact the department and are not discussed in this analysis.

PURPOSE OF BILL

According to the author's office, the purpose of this bill is to strengthen existing breach of security of personal information laws.

EFFECTIVE/OPERATIVE DATE

If enacted in the 2009 Legislative Session, this bill would be effective on January 1, 2010, and operative for notifications of a breach of security occurring on or after that date.

ANALYSIS

FEDERAL/STATE LAW

Current federal and state law provides that returns and tax information are confidential and prohibit disclosure 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, which can result in fines, imprisonment, and loss of employment or demotions. Improper disclosure of federal tax information is punishable as a felony and improper disclosure of state tax information is punishable as a misdemeanor.

Brian Putler, FTB Contact Person (916) 845-6333 (Office)	Executive Officer Selvi Stanislaus	Date 09/08/09
---	---------------------------------------	------------------

State agencies are required 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 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 a state agency to make notification 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.

The Statewide Information Management Manual (SIMM) requires agencies with systems that maintain personal information to provide an incident report within ten days to the California Highway Patrol and OPP if a breach of the system has occurred.

THIS BILL

This bill would change existing breach of security notification requirements to require the notice to be written in plain English and include the following information in the notices issued by a state agency to a California resident:

- Name and contact information of the reporting agency subject to breach and notification requirement.
- A list of the types of personal information, as defined, that were, or are, reasonably believed to have been subject to a breach.
- If the information is possible to determine at the time the notice is provided, then any of the following: the date, estimated date, or date range within which the breach occurred.
- The date of the notice.
- Whether the notification was delayed because of a law enforcement investigation if that information is available at the time the notice is provided.

- A general description of the breach incident, if that information is possible to determine at the time of the notice.
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or driver's license or California identification card number.

This bill would provide that at the discretion of the state agency, the notice may include the following additional 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.

This bill would provide that any agency that must issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification excluding any personally identifiable information to the Attorney General. The bill would specify that the notice provided to the Attorney General would not be excludable from Public Records Act requests.

This bill would also provide that if a state agency uses substitute notice, notification must be sent to the Office of Information Security within the Office of the Chief Information Officer.

LEGISLATIVE HISTORY

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 (OISPP) 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.

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 A for the complete veto message.)

SB 364 (Simitian, 2007/2008) would have required that when a state agency, subject to certain payment data related restrictions, has to notify a California resident of a breach of security of a system containing personal information, the agency must also notify the owners or licensees of the personal information subject to the breach. Governor Schwarzenegger vetoed SB 364. (See Appendix A for the complete veto message.)

SB 852 (Bowen, 2005/2006) would have expanded notice requirements to taxpayers on security breaches of personal information from only computerized data to all forms of data maintained by agencies and businesses. This bill did not pass out of the Assembly Committee on Business and Professions.

SB 1279 (Bowen, 2003/2004) would have required a state agency to provide a credit monitoring service to a person whose personal information was or may have been acquired by an unauthorized person due to a breach of security in a state agency's computer system. This bill did not pass out of the Assembly Committee on Business and Professions.

AB 700 (Simitian, Stats. 2002, Ch. 1054) established the notice requirements for breach of security of systems containing personal information.

OTHER STATES' INFORMATION

Review of *Illinois, Massachusetts, Michigan, Minnesota, and New York* found that these states have similar laws relating to the protection of personal information. All of these states used the California laws as a starting point in shaping their own laws. These states were reviewed because of the similarities between California income tax laws and their tax laws.

FISCAL IMPACT

Implementing this bill would not significantly impact the department programs or operations.

ECONOMIC IMPACT

The provisions of this bill would not impact state income tax revenues.

Appointments

None.

Support/Opposition

According to the Assembly Committee on the Judiciary analysis of June 30, 2009, the following support and opposition are noted:

Support

California Public Interest Research Group (CALPIRG)
California School Employees Association
Consumer Federation of California
Privacy Rights Clearinghouse

Opposition

Association of California Insurance Companies
Association of California Life & Health Insurance Companies
California Bankers Association
California Business Properties Association
California Chamber of Commerce
California Credit Union League (unless amended)
California Financial Services Association
California Mortgage Bankers Association
Personal Insurance Federation of California
Securities Industry and Financial Markets Association
State Farm
State Privacy and Security Coalition
Tech America

VOTES

Assembly Floor – Ayes:56 , Noes: 13
Senate Floor – Ayes: 26, Noes: 9
Concurrence – Ayes: 31 , Noes: 7

LEGISLATIVE STAFF CONTACT

Deborah Barrett
Franchise Tax Board
(916) 845-4301
deborah.barrett@ftb.ca.gov

Patrice Gau-Johnson
Franchise Tax Board
(916) 845-5521
patrice.gau-johnson@ftb.ca.gov

APPENDIX A

VETO MESSAGES FROM PRIOR LEGISLATIVE BILLS

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

BILL NUMBER: SB 364
VETOED DATE: 09/30/2008

To the Members of the California State Senate:

I am returning Senate Bill 364 without my signature.

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. The law has also provided a window on information privacy and security practices that has led organizations to make many improvements.

Unfortunately, this bill could lead consumers to believe that all data breaches result in identity theft. Further, this would place an additional unnecessary cost on businesses without a corresponding consumer benefit.

For these reasons I am unable to sign this bill.

Sincerely,

Arnold Schwarzenegger