Franchise Tax Board

ANALYSIS OF AMENDED BILL

Author: Peace | Analyst: Darrine Distefano | Bill Number: SB 1386

Related Bills: See Legislative History | Telephone: 845-6458 | Amended Date: August 5, 2002

Attorney: Patrick Kusiak | Sponsor:

SUBJECT: State Agencies Disclose Any Breach of Security of Computer Data Systems That Contain Personal Information

SUMMARY

This bill would require a state agency to notify an individual whose personal information has been accessed due to a breach of security of that agency's computer system.

This analysis does not address the bill's provisions regarding businesses or individuals since those provisions do not impact the Franchise Tax Board (FTB).

SUMMARY OF AMENDMENTS

The June 6th amendments deleted the bill's provisions relating to the California Public Records Act and added the provisions discussed in this analysis.

The June 20th amendments made the following changes to the bill:

- Specified that an agency would be required to disclose a breach of security immediately, instead of as soon as practicable, to a person whose personal information has been or was considered to be accessed by an unauthorized person.
- Added that an agency would not be required to notify a person immediately if it would impede a criminal investigation. Notification would be made as soon as the law enforcement agency determines it would not compromise the investigation.
- Added that disclosure of only the name, address, and telephone number of a person would not require an agency to notify that person of the breach.

The June 30th amendments added urgency language due to the incident at Stephen P. Teal Data Center where the financial information of state workers was put at risk for identity theft. Presently an entity is not required to notify individuals when the security of its computer database has been compromised.

The July 25th amendments made the following changes to the bill:

- Changed the timeframe during which an agency is required to disclose a breach of security.
- Required an agency that maintains personal information in a data system it does not own to notify the owner or licensee of that data system of the breach of the security of the data.
- Added definitions for several terms.

Board Position:			Department Director	Date
____ S	____ NA	____ NP		
____ SA	____ O	____ NAR	Gerald H. Goldberg	8/15/02
____ N	____ OUA	__X__ PENDING		

- Established the type of notification that an agency must provide to individuals when a breach has occurred.
- Specified that an agency that maintains its own notification procedures consistent with the timing requirements established when a breach occurs will be in compliance with the provisions of this bill.

The August 5th amendments make the following changes to the bill:

- Removes the immediate timeframe for disclosing any breach of the security of the system.
- Corrects a technical concern that the affected class of persons to be notified is 500,000 persons, not dollars.
- Makes various other technical changes.

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

PURPOSE OF THE BILL

According to the author's staff, the purpose of this bill is to require businesses and state agencies to notify an individual immediately when an unauthorized person accesses certain personal information. This warning will allow the individual to take immediate action to protect and correct, if necessary, their credit and financial accounts.

EFFECTIVE/OPERATIVE DATE

This bill is an urgency measure. It is effective and operative immediately upon enactment.

POSITION

Pending.

ANALYSIS

FEDERAL/STATE LAW

In October 1998, the federal government passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act). The Identity Theft Act creates a crime for knowingly and willingly transferring or using the identity of another person with intent to commit or aid certain unlawful activities.

Under federal law, it is a felony for a federal officer or employee to willfully disclose any tax return and return information. Punishment is a fine not to exceed $5,000 or imprisonment of no more than five years or both. Upon conviction, a federal employee is dismissed from employment. State employees and contractors who have access to federal return information are also subject to the prosecution for the same crime.

In addition, to prevent unauthorized browsing by federal officers and employees in 1997 the federal Taxpayer Browsing Protection Act (Act) was enacted. The Act creates a misdemeanor under the Internal Revenue Code for the willful, unauthorized inspection of tax returns or return information.

This Act applies to all federal employees, as well as state employees and contractors who receive federal tax information. The penalty is a fine of up to $1,000 or imprisonment up to one year or both. Upon conviction, a federal employee is dismissed from employment.

Under the California Penal Code, any person who without permission accesses the computer, computer system, or computer data of an individual, a business, or a governmental agency is subject to criminal prosecution. Depending on the type of violation, the penalty is either a felony or misdemeanor. This statute protects individuals, businesses, and government agencies from persons who without authorization tamper, interfere, damage, and access computers, computer data, and computer systems.

The California Information Practices Act (IPA) allows individuals to access information pertaining to them in state agency records. If an agency does not maintain an individual's information accurately, does not comply with an individual's request for information, or violates any provisions of the IPA, that individual may bring a civil action against the state agency.

The Revenue & Taxation Code (R&TC) prohibits the unauthorized inspection or unwarranted disclosure of any taxpayer information, except as specifically authorized by statute. Unauthorized inspection and unwarranted disclosure of state tax information is a misdemeanor. In addition, employees are subject to disciplinary action or loss of employment or both under the Civil Service Act.

THIS BILL

This bill would require an agency that owns or licenses computerized data that contains personal information to disclose when a breach of security of the system has occurred. 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. This disclosure must be made in the most expedient time possible without unreasonable delay to any individual whose unencrypted personal information was or may have been accessed by an unauthorized person.

Notification can be delayed if a law enforcement agency determines it would impede a criminal investigation. However, notification must be made once it has been determined that it would not interfere with the investigation. Notification can also be delayed if consistent with agency measures to determine the scope of the breach and to restore the integrity of the data system.

This bill would define "breach of the security of the system" as unauthorized access to computerized data that would compromise the security, confidentiality, or integrity of personal information.

This bill defines "personal information" as a person's first and last name in combination with one or more of the following: social security number; driver's license number or California Identification Card number; or 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.

This bill requires notification to be made by any of the following methods: written, electronic, or substitute notice. A substitute notice can be made if the agency demonstrates that the costs to provide the notice would exceed $250,000, or that the affected class of persons exceeds 500,000, or when the agency does not have sufficient contact information. The substitute notice will consist of all of the following: an e-mail notice when the agency has the e-mail addresses for the subject persons, the conspicuous posting of the notice on the agency's Web site, and notification to major statewide media.

This bill states that any agency that maintains its own notification procedures as part of their own information security policy will be in compliance with this bill if persons are notified in accordance with those procedures and those procedures are consistent with the timing requirements of Part 4 of the Civil Code.

IMPLEMENTATION CONSIDERATIONS

FTB has extensive firewalls to protect taxpayer data. The firewalls are updated continually as needed, and the department does not anticipate significant concerns implementing this bill.

It is unclear if the terms "unauthorized person" and "unauthorized access" would include an employee who accidentally or inappropriately accesses an individual's personal information while performing their duties. A definition of the terms "unauthorized person" and "unauthorized access" would be helpful.

The R&TC includes specific laws related to unauthorized disclosure and unwarranted inspection of confidential taxpayer information as discussed above in Federal/State Law. It is unclear how the provisions of this bill would interact with these R&TC provisions.

The bill uses the term "licenses" to describe computerized data. The author may wish to define the term "license" for clarification.

TECHNICAL CONSIDERATIONS

In referring to an agency being in compliance with this bill, the language of the bill refers to Part 4 of the Civil Code. Part 4 of the Civil Code is very broad and covers many areas that the department is unclear would be relevant to this bill. Perhaps the language of the bill should refer to Title 1.8 of Part 4 concerning personal data.

LEGISLATIVE HISTORY

AB 700 (Simitian, 2001/2002) is identical to this bill except it would be effective January 1, 2003. AB 700 is currently in the Senate Judiciary Committee.

SB 1365 (Murray, 1999/2000) would have created the "Identify Theft Victim's Protection Act," which would have made it a felony or misdemeanor to intentionally disclose personal information about a California resident to a third party for direct marketing purposes. This bill failed passage from the Senate Committee on Public Safety.

SB 1383 (Leslie, Stats. 1998, Ch. 623) established the misdemeanor crime for any willful unauthorized inspection including unwarranted disclosure or use of confidential information of confidential taxpayer information by an employee, deputy, agent, clerk, other officer, or member of the FTB. This act is also called the Taxpayer Browsing Protection Act.

AB 2883 (Caldera, Stats. 1994, Ch. 91) and AB 1040 (Committee on Revenue and Taxation, Stats. 1997, Ch. 605) established the misdemeanor crime for the disclosure of any confidential taxpayer and business corporation information.

PROGRAM BACKGROUND

The Office of Personnel Management in federal government has prescribed regulations to administer the federal laws for unauthorized browsing cases. These regulations allow an adverse personnel action to be taken against a federal officer or employee who violates federal policies, rules, regulations, and laws. These regulations authorize a federal agency to take one of the following adverse actions against a federal employee:

- Suspend the employee temporarily without pay or duties,
- Remove the employee from federal employment, or
- Reduce the employee's grade or pay.

Based on existing state civil service and privacy laws, it is normal practice for state agencies, including the FTB, to take formal adverse personnel action against employees who engage in misconduct by violating consumer, citizen or taxpayer privacy protections.

OTHER STATES' INFORMATION

Review of statutes for *Illinois, Massachusetts, Michigan, and Minnesota* found laws similar to the federal laws for unauthorized inspection or unwarranted disclosure of personal information. However, it is not known if notification is sent to individuals when a breach of a state agency's database has occurred.

These states were reviewed because of the similarities between California income tax laws and their tax laws.

FISCAL IMPACT

If notification is required only when an *intentional* access (including unauthorized employee access) is made, it is estimated that the department will need 3 personnel years (PYs) at a total cost of $241,000 to $262,000 per year to notify and respond to taxpayers.

Due to budget constraints, the department would request appropriations be attached to the bill to support the positions necessary to properly implement the provisions of this bill.

ECONOMIC IMPACT

This bill would not impact the state's income tax revenue.

POLICY CONSIDERATIONS

The R&TC relating to unauthorized inspection and disclosure is based on the browsing and disclosure laws within the Internal Revenue Code (IRC). While the IRC includes provisions requiring the dismissal or discharge of federal officers and employees upon conviction for the willful, unauthorized inspection of income tax returns or return information, the R&TC does not conform to this provision for state employees.

LEGISLATIVE STAFF CONTACT

Darrine Distefano
Franchise Tax Board
845-6458
Darrine.Distefano@ftb.ca.gov

Brian Putler
Franchise Tax Board
845-6333
Brian.Putler@ftb.ca.gov