

ANALYSIS OF AMENDED BILL

Franchise Tax Board

Author: Jones Analyst: Deborah Barrett Bill Number: AB 779

Related Bills: See Legislative History Telephone: 845-4301 Amended Date: May 14, 2007

Attorney: Patrick Kusiak Sponsor: _____

SUBJECT: State Agencies Notify California Resident & Office Of Privacy Protection Of Breach in Security Of Data/Required Information To Be Included In Notification

SUMMARY

This bill would do the following:

- prohibit certain state agencies from retaining payment related data, and
- require that the Office of Privacy Protection (OPP) be provided a copy of the notice sent to California residents when a breach of security of a system containing personal information has occurred.

SUMMARY OF AMENDMENTS

The May 14, 2007, amendments added provisions that would prohibit the retention of payment related data and removed restrictions relating to retention of personal information by retail sellers. The May 14, 2007, amendments also added minimum information that must be included in a notice to a California resident of a breach of the security of a system containing personal information and a requirement that OPP receive a copy of the notice sent to the resident.

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

PURPOSE OF THE BILL

According to the author's staff, the purpose of the bill is to improve the quality of the notices issued for a breach of security, to implement industry standards to safeguard sensitive data, including not collecting unnecessary data to begin with, and to provide an incentive to protect the data by providing a reimbursement mechanism if data is breached.

EFFECTIVE/OPERATIVE DATE

This bill would be effective January 1, 2008, and operative for security breaches that occur on or after that date.

POSITION

Pending.

Board Position:	Department Director	Date
<input type="checkbox"/> S		
<input type="checkbox"/> SA		
<input type="checkbox"/> N		
<input type="checkbox"/> NA		
<input type="checkbox"/> O		
<input type="checkbox"/> OUA		
<input type="checkbox"/> NP		
<input type="checkbox"/> NAR		
<input checked="" type="checkbox"/> PENDING	Selvi Stanislaus	6/15/07

ANALYSIS

FEDERAL/STATE LAW

Under federal law, financial institutions are prohibited from disclosing the nonpublic personal information of their customers to a nonaffiliated third party unless they have provided notice as specified that such information may be disclosed to the third party.

Current federal and state law provides that 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 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 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 prohibit a person, business, or state agency that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device from storing payment related data, except as specified. If the person, business, or state agency has established a payment data retention and disposal policy that limits the amount of payment related data and the time that data is retained to the amount and time required for business, legal or regulatory purposes and is documented in the payment data retention policy, the prohibition does not apply.

This bill would also prohibit the following:

- storage of sensitive authentication data subsequent to authorization,
- storage of any payment related data that is not needed for business purposes,
- retention of the primary account number unless retained in a manner consistent with other provisions of the bill and in a form that is expected to be indecipherable by unauthorized users,
- sending payment related data across any network unless the data is encrypted using strong cryptography and security,
- allowing access to payment related data by any individual whose job does not require that access.

The provisions of this bill are not applicable to financial institutions that are in compliance with federal regulations relating to disclosure of nonpublic information and are subject to compliance oversight by a state or federal regulatory agency with respect to those regulations.

The bill's definition of authentication data includes, but is not limited to, all of the following:

- The full contents of any data track from a payment card or other payment device.
- The card verification code or any value used to verify transactions when the payment device is not present.
- The personal identification number (PIN) or the encrypted PIN block.

This bill would amend existing breach of security of personal data laws in the following ways:

1. Require that notices be written in plain language,
2. Require notices to include the following information:
 - The date of the notice.
 - The name of the agency that maintained the computerized data at the time of the breach.
 - The date or estimate of the date the breach occurred if the breach is possible to determine.
 - A description of the categories of personal information that were or are reasonably believed to have been acquired by an unauthorized person.

- A toll-free telephone number for the agency subject to the breach of the security of that agency's system or if the primary method used by that agency to communicate with the individual is by electronic means, an electronic mail address that the individual may use to contact the agency so that the individual may learn what types of personal information that agency maintained about the individual was subject to the security breach. If the agency does not have a toll-free number, a local telephone number may be provided to a California resident to contact the agency.
 - The toll-free telephone numbers and addresses for the major credit reporting agencies,
3. Require that a copy of the notice sent to the California resident be provided to the OPP, and
 4. Require that the owner of the personal information is entitled to be reimbursed from the agency that maintained the computerized data for all reasonable and actual costs of providing notice to consumers regarding the breach of the security of the system. Reasonable and actual costs include but are not limited to the costs of card replacement as a result of the breach of the security of the system.

This bill would also repeal duplicative sections.

PROGRAM BACKGROUND

FTB maintains a data retention policy for personal information that includes return information, which in turn includes payment related data. Retention time-frames vary from no less than the minimum amount of time required by law to seven years from the later of the original due date of the income tax return or the date the original, or an amended tax return was filed.

Additionally, FTB does not accept debit card payment transactions, unless the debit cards can be used interchangeably as credit cards. An alternative electronic payment option offered by the department is Web Pay. Web Pay is an online application that can be used to make electronic withdrawals from taxpayers' checking or savings accounts to pay their personal income taxes. The payment can be scheduled up to one year in advance. Credit card payments are accepted for tax payments, but are not currently available for use in the non-tax debt programs the department administers.

IMPLEMENTATION CONSIDERATIONS

The department has identified the following implementation concerns. Department staff is available to work with the author's office to resolve these and other concerns that may be identified.

Because the majority of FTB's transactions with taxpayers are payments of tax obligations, rather than purchases of goods or services, the department would interpret the bill's provisions to have no application to FTB. If it is the author's intention that these requirements apply to tax payments made to FTB, it is recommended that payments for purposes other than goods and services be expressly included.

The department is prohibited from disclosing return information, such as names and addresses that would be on the notices required to be sent to OPP. Based on discussion with the author's staff, the bill should be revised to specify that a sample of the notice sent in the event of a breach of security be provided so that OPP can have sufficient information to assist residents.

The bill requires notice to be sent when a breach of a system containing "unencrypted" personal information occurs, but requires the notice to contain sufficient information to identify the person whose "encrypted" personal information was or may have been acquired by an authorized person. It is suggested that the inconsistency between the trigger that requires notification and the content of the notice should be made consistent.

LEGISLATIVE HISTORY

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 did not pass out of the Senate Business and Professions 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 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 remained with the Assembly Business and Professions Committee.

AB 700 (Simitian, Stat. 2002, Ch. 1054) requires a state agency to notify residents 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.

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 accept payment by credit card and use intermediaries to assist in the processing of the transactions. *Minnesota* charges a convenience fee directly to the taxpayer, and then remits that fee to the service provider. The other states' arrangements parallel California's.

All of these states have statutes for the breach of systems containing personal information similar to California's. 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

Because the department is unable to predict when a breach of security may happen or how extensive that breach may be, the costs that would be incurred to reimburse an owner of data is unknown. If the implementation considerations addressed in this analysis are resolved, 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

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

Brian Putler
Franchise Tax Board
(916) 845-6333
brian.putler@ftb.ca.gov