

ANALYSIS OF AMENDED BILL

Franchise Tax Board

Author: Jones Analyst: Deborah Barrett Bill Number: AB 1656

Related Bills: See Legislative History Telephone: 845-4301 Amended Date: August 6, 2008

Attorney: Patrick Kusiak Sponsor: _____

SUBJECT: State Agencies Notify California Residents Of Breach In Security Of Data/Notice Requirement If Substitute Notice Is Utilized, Provide To Office Of Privacy Protection

SUMMARY

This bill would do the following:

- Establish payment related data retention requirements for specified state agencies,
- Require state agencies to provide specific information when notifying owners and licensees of personal information of a breach of security of a system containing personal information, and
- Provide that when substitute notice is used, a notice must be sent to the Office of Information security and Privacy Protection (OISPP).

SUMMARY OF AMENDMENTS

The August 6, 2008, amendments would do the following:

- Remove provisions in the Education Code relating to pupil achievement.
- Establish payment-related data retention requirements for state agencies that accept credit cards, debit cards, or other payment devices in the sale of goods or services.
- Require that when state agencies provide a notice to the owners or licensees of the personal data involved in the breach, specific information is required to be included in the notice.
- Identify specified information in the notice sent to owners or licensees of data.
- Require notification to the OISPP be provided when substitute notice is used.
- Make the provisions of the bill operative only if SB 364 of the 2007-08 Regular Session is enacted and takes effect on or before January 1, 2009.

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

Board Position:

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

Department Director

Date

Selvi Stanislaus

8/29/08

PURPOSE OF THE BILL

According to the author's office, the purpose of this 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, 2009, and as specified in the bill, would be operative only if SB 364 of the 2007-2008 Regular Session is enacted and takes effect on or before January 1, 2009.

POSITION

Pending.

ANALYSIS

STATE LAW

Under current state law, any agency that owns or licenses computerized data that includes personal information and experiences a breach of security of the system containing that data must notify the affected individuals that their unencrypted information may have been acquired by an unauthorized person. Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. Notification of the breach of security can be provided by written notice, electronic notice, or substitute notice if the cost of providing the notice would exceed \$250,000 or involves a class of affected persons in excess of 500,000 persons. Substitute notice would be accomplished by e-mail notification, posting of the notice in a conspicuous place on the agency's web site, or notifying major statewide media.

THIS BILL

This bill would prohibit, with certain exceptions, a person, business, or state agency (entity) 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. The bill would require the entity to have a data retention and disposal policy that limits the amount of payment-related data and the time that data is retained to only the amount and time required for business, legal, or regulatory purposes and to explicitly document such in the policy.

This bill would also prohibit the following:

- Storage of sensitive authentication data, as defined, subsequent to authorization,
- Storage of any payment related data that is not needed for business, legal, or regulatory purposes,
- Storage of any of the following data elements:
 - Payment verification code
 - Payment verification value
 - PIN verification value
- Retention of the primary account number unless retained in a manner consistent with other provisions of the bill and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored,
- Sending payment related data across any open public network unless the data is encrypted using strong cryptography and security protocols or otherwise rendered indecipherable, and
- Allowing access to payment related data by any individual whose job does not require that access.

Sensitive 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

The provisions of this bill are not intended to prohibit an entity from storing payment-related data for the sole purpose of processing ongoing or recurring payments, provided that the payment-related data is maintained in accordance with the requirements of the bill.

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

This bill would require an entity subject to the payment-related data restrictions that is required to notify the owners or licensees of the data if an unauthorized person breaches the system containing that data to include specific information in the notice. The specific information required in the notice, if available at the time the notice is provided, includes:

- The date of the notice
- The name of the entity that maintained the computerized data
- The date, estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided.
- A description of the categories of personal information that was, or is reasonably believed to have been, acquired by an unauthorized person.

- A toll-free number for the entity subject to the breach of the security of the system, or under specified circumstances, an e-mail address where the entity can be reached so the individual may learn what types of personal information that entity maintained. If the entity does not have a toll-free telephone number, a local number may be provided.
- The toll-free telephone numbers and addresses for the major credit reporting agencies.

The notice can be delayed if a law enforcement agency determines that the notice would impede a criminal investigation. Notice in those circumstances would be made after a law enforcement agency determines that the notice would not impede the criminal investigation.

This bill would require owners or licensees of the payment related data that receives a notice under the provisions of the bill to disclose to the California resident in any notice they provide the same information provided to them by the entity that experienced the breach of security.

This bill would provide that if notice is required, the agency whose system was breached is liable to the owner or licensee of the information for the reimbursement of actual costs of providing notice to consumers regarding the breach of the security of the system.

This bill would require that if substitute notice as authorized is provided, the OISPP must also be notified.

The provisions of this bill would make the bill operative only if SB 364 of the 2007-2008 Regular Session is enacted and takes effect on or before January 1, 2009.

IMPLEMENTATION CONSIDERATIONS

The provisions of this bill apply to state agencies that accept credit cards, debit cards, or other payment devices when conducting sales of goods or service. Accordingly, FTB would interpret the provisions of this bill not to apply to transactions where a taxpayer pays their income tax obligation. If the author seeks a different result, the author may want to add payment of obligations in the type of transaction that would be subject to the additional notice requirements established under the provisions of this bill.

LEGISLATIVE HISTORY

AB 1779 (Jones 2008) would prohibit a state agency from retaining payment related data and would require 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 has been referred to the Senate Judiciary Committee.

SB 364 (Simitian, 2007/2008) bill would require 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. SB 364 is currently in the Senate Appropriations 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. AB 779 was vetoed by Governor Schwarzenegger. (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.

PROGRAM BACKGROUND*

FTB maintains a data retention policy for personal information that includes return information, including 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 tax return or the date the original or an amended tax return was filed.

FTB does not accept debit card payment transactions, unless the debit cards can be used interchangeably as credit cards. The other 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 tax. 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.

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 OISPP if a breach of the system has occurred.

OTHER STATES' INFORMATION

Review of *Illinois, Massachusetts, Michigan, Minnesota, and New York* found that these states have laws similar to California's existing law relating to the protection of personal information. All of these states used the California laws¹ as a starting point in shaping their own laws, but do not have provisions similar to this bill's in their existing law. These states were reviewed because of the similarities between California income tax laws and their tax laws.

¹ Civil Code Sections 1798.29 – 1798.84

FISCAL IMPACT

Because FTB does not store payment related data therefore eliminating the potential of payment related data from being acquired by unauthorized persons, implementing this bill would not impact department costs.

ECONOMIC IMPACT

This bill would not impact state income tax revenues.

POLICY CONCERNS

Because current SIMM instructions require state agencies that maintain systems containing personal information to provide an Incident Report to OPP within ten days of the incident, the similar provisions of this bill, as they relate to state agencies, are duplicative.

LEGISLATIVE STAFF CONTACT

Legislative Analyst

Deborah Barrett

(916) 845-4301

Deborah.Barrett@ftb.ca.gov

Revenue Manager

Rebecca Schlussler

(916) 845-5986

rebecca.schlussler@ftb.ca.gov

Legislative Director

Brian Putler

(916) 845-6333

brian.putler@ftb.ca.gov

Appendix A

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