

**SUMMARY ANALYSIS OF AMENDED BILL**

Author:  Jones  Analyst:  Deborah Barrett  Bill Number:  AB 779   
 Related Bills:  See Prior Analysis  Telephone:  845-4301  Amended Date:  June 1, 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

\_\_\_\_\_ DEPARTMENT AMENDMENTS ACCEPTED. Amendments reflect suggestions of previous analysis of bill as introduced/amended \_\_\_\_\_.

\_\_\_\_\_ AMENDMENTS IMPACT REVENUE. A new revenue estimate is provided.

\_\_\_\_\_ AMENDMENTS DID NOT RESOLVE THE DEPARTMENT'S CONCERNS stated in the previous analysis of bill as introduced/amended \_\_\_\_\_.

\_\_\_\_\_ FURTHER AMENDMENTS NECESSARY.

\_\_\_\_\_ DEPARTMENT POSITION CHANGED TO \_\_\_\_\_.

\_\_\_\_\_ REMAINDER OF PREVIOUS ANALYSIS OF BILL AS AMENDED  May 17, 2007 , STILL  X  APPLIES.

\_\_\_\_\_ OTHER – See comments below.

**SUMMARY**

This bill would do the following:

- Prohibit a state agency from retaining payment related data, and
- Require that the Office of Privacy Protection (OPP) be provided a copy of the substitute notice issued when a breach of security of a system containing personal information has occurred.

**SUMMARY OF AMENDMENTS**

The June 1, 2007, amendments revised the requirement that OPP be provided a copy of the notice of a breach of security of a system containing personal information and limited the requirement to apply only in instances when substitute notice is issued. The June 1, 2007, amendments also removed the prohibition for payment related data being sent across any network and modified it to prohibit unencrypted payment related data from being sent over open public networks. The amendments did not resolve all of the "Implementation Concerns" identified in the department's analysis of the bill as amended May 17, 2007; the unresolved concern is restated here for convenience. The "This Bill" and "Fiscal Impact" discussion have been revised. The remainder of the department's analysis of the bill as amended May 17, 2007, still applies.

Board Position:	Legislative Director	Date
_____ S		
_____ SA	Brian Putler	7/10/07
_____ N		
_____ NA		
_____ O		
_____ OUA		
_____ NP		
_____ NAR		
_____ X PENDING		

## **POSITION**

Pending.

## **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 that is 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 open public 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 also require that if notice is required, the person, business, or public agency whose system was breached is liable to the owner or licensee of the information for the reimbursement of 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 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, and
3. 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 require that if substitute notice as authorized is provided, OPP must also be notified.

This bill would also repeal duplicative sections.

#### IMPLEMENTATION CONSIDERATION

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

Because the majority of Franchise Tax Board's (FTB) 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.

## **FISCAL IMPACT**

The department is unable to determine the extent of the costs that may be associated with a security breach that would require the department to reimburse an owner of data. Although FTB expends considerable resources protecting taxpayer data, the cost to mitigate the impact of a security breach exposing millions of taxpayer records to an unauthorized user would be substantial.

## **LEGISLATIVE STAFF CONTACT**

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

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