

**SUMMARY ANALYSIS OF AMENDED BILL**

Author: Jones Analyst: Deborah Barrett Bill Number: AB 779  
 Related Bills: See Prior Analysis Telephone: 845-4301 Amended Date: July 10, 2007  
 Attorney: Patrick Kusiak Sponsor: \_\_\_\_\_

|  |  |
|--|--|
| <b>SUBJECT:</b>  | State Agencies Notify California Resident & Office Of Privacy Protection Of Breach in Security Of Data/Required Information To Be Included In Notification |
| <p><input type="checkbox"/> DEPARTMENT AMENDMENTS ACCEPTED. Amendments reflect suggestions of previous analysis of bill as introduced/amended _____.</p> <p><input type="checkbox"/> AMENDMENTS IMPACT REVENUE. A new revenue estimate is provided.</p> <p><input checked="" type="checkbox"/> AMENDMENTS DID NOT RESOLVE THE DEPARTMENT'S CONCERNS stated in the previous analysis of bill as amended <u>July 3, 2007</u>.</p> <p><input type="checkbox"/> FURTHER AMENDMENTS NECESSARY.</p> <p><input type="checkbox"/> DEPARTMENT POSITION CHANGED TO _____.</p> <p><input checked="" type="checkbox"/> REMAINDER OF PREVIOUS ANALYSIS OF BILL AS AMENDED <u>July 3, 2007</u>, STILL APPLIES.</p> <p><input type="checkbox"/> OTHER – See comments below.</p> |  |

**SUMMARY**

This bill would prohibit a state agency that sells goods or services from retaining payment related data and would require certain information to be included in notices related to a breach of security issued by state agencies subject to the payment related data requirements.

**SUMMARY OF AMENDMENTS**

The July 10, 2007, amendments would do the following:

- Require that under certain circumstances, a state agency must provide specific information to owners or licensees of payment related data when a breach of security of the system containing that data has occurred, and
- Remove the specific items of information required to be in a notice to California residents sent by a state agency in the event of a breach of security.

|   |   |         |
|---|---|---------|
| Board Position:                             | Legislative 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 | Patrice Gau-Johnson<br>for Brian Putler | 7/31/07 |

The July 10, 2007, amendments resolved the "Technical Consideration" identified in the department's analysis of the bill as amended July 3, 2007, but did not resolve the "Implementation Consideration" identified in the same analysis. The "Implementation Consideration" and "This Bill" discussions have been revised. The remainder of the department's analysis of the bill as amended July 3, 2007, still applies.

## **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. This prohibition does not apply if the person, business, or state agency has done the following:

- Established a payment data retention and disposal policy that limits the amount of payment related data,
- Limited the time that data is retained to the amount and time that is required for business, legal or regulatory purposes, and
- Documented the time retention periods in the payment data retention policy.

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, and
- 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 require those agencies subject to the payment related data restrictions to notify the owners or licensees of the data if the system containing that data has been breached by an unauthorized person. 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 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 the notices to the owners or licensees of the payment related data to comply with the following specifications:

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. If the owner or licensee of the information is the issuer of the credit or debit card or the payment device, or maintains the account information from which the payment device orders payment, the owner or licensee must disclose to the California resident the information provided for in this bill.

This bill would provide 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, The Office of Privacy Protection must also be notified.

This bill would also repeal duplicative sections.

## IMPLEMENTATION CONSIDERATIONS

Because the majority of the 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 related to the retention of payment related data to have no application to FTB. Consequently, because the July 10, 2007, amendments make the requirement to notify owners or licensees of data in the event of a security breach conditioned upon being subject to the retention of payment related data requirements, the July 10, 2007, amendments do not apply to FTB either. 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.

## **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)