

DEPARTMENT OF FINANCE BILL ANALYSIS

AMENDMENT DATE: July 7, 2009
POSITION: Neutral

BILL NUMBER: SB 20
AUTHOR: J. Simitian
RELATED BILLS: None

BILL SUMMARY: Personal Information: Privacy

This bill amends current security breach notification law as specified in Sections 1798.29 and 1798.82 of the Civil Code. These sections apply to state agencies, persons or businesses conducting business in California that own or license computerized data that includes personal information. The bill has three components:

- 1. Specify security breach notices be written in plain language and include certain standard information such as: reporting agency contact information; type of information believed to have been breached; date or date range of incident and date of notice; if notification was delayed due to a law enforcement investigation; description of the incident; estimated number of persons affected; and credit agency contact information.
2. Require the Attorney General (AG) be notified if more than 500 California residents are affected by a single breach.
3. Require the Office of Information Security (OIS) within the Office of the State Chief Information Officer (OCIO) and the Office of Privacy Protection (OPP) within the State and Consumer Services Agency be notified if the substitute notice provision in current law is used as notification. Substitute notice consists of e-mail, Internet website posting, and notifying major statewide media. Substitute notice is permitted if the costs would exceed \$250,000, the number of persons exceeds 500,000, or if the agency does not have sufficient contact information.

SUMMARY OF CHANGES

Amendments to this bill since our analysis of the March 4, 2009 version are minor and do not alter our position:

- The requirement that the agency provide the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a bank account or credit card number has been removed.
Language has been added to specify that the standard information required to be included in the notification shall be included if that information is possible to determine at the time the notice is provided.
References to the Office of Information Security and Privacy Protection (OISPP) have been updated to reflect the Governor's IT Reorganization Plan. The OISPP has been replaced by the OIS within the OCIO and the OPP within the State and Consumer Services Agency. For clarity, references to the OISPP have been updated throughout this analysis to reflect this change.

Analyst/Principal Date Program Budget Manager Date
(0843) R. Gillihan Diana Ducay

Department Deputy Director Date

Governor's Office: By: Date: Position Approved
Position Disapproved

BILL ANALYSIS Form DF-43 (Rev 03/95 Buff)

J. Simitian

July 7, 2009

SB 20

**FISCAL SUMMARY****Specified Content for Security Breach Notifications**

There may be additional staff resources necessary to collect the information required for the breach notification. The extent of the additional amount of staff resources is unknown. Finance contacted the Department of Health Care Services (DHCS) as a representative department that, given the size of the population they serve, would have to provide notification to large numbers of people in the event of a security breach. DHCS indicated that their notification already includes all of the standard content specified in the bill and as a state agency they are already required to notify the OIS. Their only concern was the requirement to notify the AG if more than 500 persons were impacted by the breach. DHCS pointed out that the severity of the breach should determine whether the AG is notified and, by using a set number, it is inconsistent with the security incident reporting requirements of the OIS, which are based on the nature of the incident, not the number of people impacted.

**Notification to the Attorney General**

There may be additional staff resources necessary to receive the notifications and handle them, possibly through logging them in and posting them to a website. The AG indicates this could be accomplished with existing staff resources.

**Notification to the OIS and the OPP**

The OIS and the OPP indicated that this bill would have minimal fiscal impact on their agencies. Existing policy in Section 5350.1 of the State Administrative Manual already requires state agencies to report security breaches to the OIS.

**COMMENTS**

Primarily due to the limited fiscal impact to the state, Finance is neutral regarding the three components of this bill: specified content for security breach notifications, notification to the AG, and notification to the OIS and the OPP. However, certain stakeholders and interested parties have expressed support, opposition, or concerns with the content of the bill as noted below:

- Support: The Privacy Rights Clearinghouse, a consumer advocacy group dedicated to protecting consumers against identity theft and other types of privacy crime, supports this bill. They articulated their support in a letter to Senator Simitian's office dated March 18, 2009.
- Concerned: The California Credit Union League is not opposed to the bill, but has some concerns regarding whether some of the specified content would be known at the time the notice is provided. They are in conversation with the author to possibly amend the language of the bill to provide that specified items of information must be included in the security breach notification, if available at the time the notice is provided. (This concern was addressed in the June 16 amendment to this bill.)
- Opposed: A number of groups, including the State Privacy and Security Coalition that counts Google, Yahoo, and AOL as members, are opposed to the bill as they feel that current breach notification requirements are sufficient. They are concerned that providing the date of a breach gives a hacker an opportunity to determine whether his or her attack was successful. They are also concerned that providing customers with credit agency contact information implies that all breaches result in fraud and identity theft. They expressed these concerns in a letter to the Senate Judiciary Committee dated February 12, 2009.

**Specified Content for Security Breach Notifications**

- Fiscal impact to state agencies is most likely extremely minor, if any. According to the author's staff, the bill is mainly directed at the private sector.
- Breach notifications provided by state agencies, in at least one case, already include the content specified in this bill.

J. Simitian

July 7, 2009

SB 20

**Notification to the Attorney General**

The AG does not take a position on this bill, however staff commented that most likely an e-mail address would be established to receive the notifications, which would then be posted to the AG website. Staff further commented that as statistical tracking of breaches is already performed by the OIS/OPP, it is not clear the further benefit of notifying the AG as well. Staff added that the California Highway Patrol receives breach information from state agencies, but not from the private sector.

The OPP notes that notifying the AG makes the breach a matter of public record, giving the industry access to this information which could assist policymakers by providing them with more information on the scope and nature of security breaches.

**Notification to the OIS and the OPP**

- Fiscal impact to state agencies is most likely extremely minor, if any, as they are already required to report security incidents to the OIS, regardless of whether they resulted in a breach notification.
- Fiscal impact to the OPP as a result of receiving security breach notifications from persons or businesses is unknown, but most likely minor.
- The OCIO, which houses the OIS, has indicated that it will take no position on this bill, as the bill would have limited to no impact on their agency. The OCIO believes the impact will be primarily on the agencies who own the information subject to the breach notifications.

**General Comments**

We note that, as persons and businesses are currently subject to breach notification requirements, the fiscal/non-fiscal impact of this bill on these entities would likely be minimal.

Code/Department Agency or Revenue Type	SO	(Fiscal Impact by Fiscal Year)							Fund Code
	LA	(Dollars in Thousands)							
	CO RV	PROP 98	FC	2008-2009 FC	2009-2010 FC	2010-2011 FC			
0820/Justice	SO	No			-----	No/Minor Fiscal Impact	-----	0001	
0510/Secty SCS	SO	No			-----	No/Minor Fiscal Impact	-----	0001	
0502/Chief Info	SO	No			-----	No/Minor Fiscal Impact	-----	0001	