

California Enacts Three Bills Amending Breach Notification Statute

October 15, 2015

Last week, California Governor Jerry Brown signed into law three bills that revise California's data breach notification statute. The bills, which take effect January 1, 2016, establish specific formatting requirements for the consumer breach notice letter; define "encrypted"; and create notice, security, and privacy obligations for data captured by automated license plate recognition (ALPR) systems. The enactment of these bills, and [others](#), indicates California's continued commitment to reviewing and revising privacy- and security-related legislation to address perceived gaps and new threats.

Currently, California's breach notification statute requires that the plain-language notice to affected consumers include (1) the notifying entity's name and contact information; (2) a list of the types of personal information subject to the breach; (3) the date of the breach; (4) whether notification was delayed due to a law enforcement investigation; (5) if the breach involved Social Security, driver's license, or California identification card numbers, the phone numbers and addresses of the major credit reporting agencies; and (6) if identity theft and mitigation services are offered, all information necessary to take advantage of that offer. [S.B. 570](#) adds the following formatting requirements:

1. The notice must be titled "Notice of Data Breach."
2. The required content (listed above) must be described under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
3. The format of the notice must be designed to call attention to the nature and significance of the information it contains.
4. The title and headings must be clearly and conspicuously displayed.
5. The text must be at least 10-point type.

Notices using the following model security breach notification form will be deemed to be compliant.

NAME OF INSTITUTION / LOSS		Date: (insert date)
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		
What You Can Do.		
Other Important Information. (insert other important information)		
For more information.	call (telephone number) or go to (Internet web site)	

Under California law, a breach has occurred only if the compromised personal information is not encrypted. [A.B. 964](#) defines “encrypted” as “rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.”

[S.B. 34](#) amends the definition of “personal information,” adding “information or data collected through the use or operation of an automated license plate recognition system.” Additionally, the bill requires that ALPR operators and end-users maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information, and a usage and privacy policy detailing their ALPR information collection, use, maintenance, sharing, and dissemination practices. The bill also creates a private right of action, under which individuals may bring a civil action, and a court may award actual damages of up to \$2,500, punitive damages, reasonable attorney’s fees and costs, and/or other preliminary and equitable relief.