

Privacy - New California Security Breach Notification Requirements Set Standard Core Content for Notification Letters

January 27, 2012 by [Timothy Moroney](#) and [Dawn Valentine](#)

The purpose of this alert is twofold: (1) to remind our clients that both federal and state law requires financial institutions and most businesses to safeguard their customers' information; and (2) to advise of new requirements for security breach notification letters.

In 2002, California adopted a first-in-the-nation security breach notification statute ([AB 700](#), Simitian) (the "Security Breach Notification Law").

The Security Breach Notification Law requires companies that do business in California and retain their customer's personal information to notify individuals when there has been a data breach involving their personal information.

Background

Since 2002, 45 other states, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, have also enacted security breach notification laws that are modeled upon California's Security Breach Notification Law. Only Alabama, Kentucky, New Mexico and South Dakota do not have security breach notification laws.

Moreover, 14 states (Hawaii, Iowa, Maryland, Massachusetts, Minnesota, New Hampshire, New York, North Carolina, Oregon, Vermont, Virginia, West Virginia, Wisconsin, and Wyoming) and Puerto Rico have built upon California's model and added more detailed requirements for security breach notifications to include certain types of information.

Further, the federal government has weighed in. As of February 19, 2009, for breaches of personal medical information, individuals have to be notified and those notifications must contain certain specified content.

Still further, most of these states require a business that suffers a security breach to notify a state regulator, such as the Attorney General, in addition to the affected individuals (Alaska, Hawaii, Louisiana, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, South Carolina, Vermont, and Virginia).

SB 24 Data Breach Notification

Accordingly, not to be outdone as the leader in consumer protection, effective January 1, 2012, California adopted new requirements ([SB 24](#) – amending Civil Code sections

1798.29 and 1798.82) for what information must be put in a security breach notification letter.

The purpose underlying these new requirements is to close a gap that has been identified – the old requirements simply required data holders to notify individuals when there had been a data breach involving personal information but were silent on what information should be contained in the notification.

As a result, security breach notification letters varied greatly in the information provided leaving consumers confused and not providing answers to the questions of what information was breached, when did the breach occur, and what consumers should do to protect themselves.

Moreover, businesses were left exposed and uncertain of what was expected of them in the event of a breach.

The new requirements fill this gap by establishing standard, core content for the notification letters. Specifically, the new law requires that security breach notification letters, at a minimum, contain the following information:

1. The name and contact information of the reporting agency, person, or business;
2. A list of the types of personal information that was compromised or the subject of the breach;
3. Any of the following, if the information is possible to determine at the time the notice is provided: the date or estimated date of the breach, or date range within which the breach occurred;
4. The date of the notice;
5. Whether the notification was delayed because of an investigation by law enforcement, if the information is possible to determine at the time the notice is provided;
6. A general description of the breach incident, if the information is possible to determine at the time the notice is provided; and
7. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number, or a driver's license or California Identification Card number.

This new law also provides that an agency, person, or business may also include the following information in a security breach notification, at its discretion:

1. Information regarding what the entity has done to protect individuals whose information has been breached; and
2. Advice on steps that the individual may take to protect himself or herself.

The new requirements also obligate any agency, person, or business that is required to provide a security breach notification to more than 500 California residents as a result of a single breach of the security system to submit a single sample copy of the notification electronically to the California Attorney General. That copy **shall not** be considered to be a record of complaint or investigation under the [California Public Records Act](#).

The purpose of this alert is twofold: (1) to remind our clients that both federal and state law requires financial institutions and most businesses to safeguard their customers' information; and (2) to advise of new requirements for security breach notification letters.

Generally, safeguarding standards applicable to financial institutions and most businesses require the creation and implementation of a comprehensive written information security program that includes administrative, technical and physical safeguards to: (1) ensure the security and confidentiality of customer information; (2) protect against anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information.

Since security breaches catch the attention of the big media, if you are not in compliance with your safeguarding obligations now is the time to come into compliance.

If you have any questions or comments about your safeguarding obligations, please don't hesitate to contact Tim Moroney at (415) 743-3713; tmoroney@bargerwolen.com or Dawn Valentine at (415) 743-3731; dvalentine@bargerwolen.com.