Published on *The National Law Review* https://natlawreview.com

New California Law Protects Online Account Information

Article By:

Joseph Duffy

Gregory T. Parks

Ezra D. Church

W. Reece Hirsch

Carla B. Oakley

As of January 1, security breach notifications must be provided to consumers when certain account information is compromised.

On September 27, California Governor Jerry Brown signed into law Senate Bill No. 46 (S.B. 46), a new data breach notification law that expands consumer protections by requiring that security breach notifications be provided when passwords, usernames, or security questions or answers that would permit access to an online account are breached. California's existing data breach notification law requires that consumers be alerted only when a security breach has exposed Social Security numbers, driver's license numbers, credit card numbers, or medical or health insurance information. No notification is currently required when other online account information is breached. S.B. 46 will take effect on January 1, 2014.

Overview of S.B. 46

Both the existing law and the newly enacted S.B. 46 apply to any agency or any person or business that conducts business in California and owns or licenses computerized data that includes personal information. These persons or businesses are required to notify any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Specifically, S.B. 46 expands the definition of "personal information" to now include either of the following pieces of unencrypted information:

- An individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
    - Social Security number

- Driver’s license number of California identification card number
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account
- Medical information
- Health insurance information

- A username or email address, in combination with a password or security question and answer that would permit access to an online account

S.B. 46 also imposes additional requirements on the disclosure of a security breach in situations where the breach involves personal information that would permit access to an online or email account. Specifically, if the breach includes a username or email address, in combination with a password or security question and answer that would permit access to an online account, and does not include any of the other information in the above definition of “personal information,” the person or business may notify the consumer in an electronic form that directs the consumer to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the business and all other online accounts for which the person uses the same username or email address and password or security question or answer.

However, if the breach includes a username or email address, in combination with a password or security question and answer that would permit access to an email account furnished by a business, the person or business must not provide the security breach notification to that email address. Instead, the person or business must comply by providing notice in one of the following methods:

- Written notice
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the U.S. Code
- Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, that the affected class of subject persons to be notified exceeds 500,000, or that the person or business does not have sufficient contact information

Substitute notice shall consist of all of the following: (a) email notice when the person or business has an email address for the subject persons; (b) conspicuous posting of the notice on the Internet website of the person or business, if the person or business maintains one; and (c) notification to major statewide media. Alternatively, clear and conspicuous notice may be delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

The law also expressly allows people and businesses to provide notice pursuant to their own notification procedures that are part of an information security policy for the treatment of personal information as long as those procedures are otherwise consistent with the timing requirements of the

statute.

Notification Requirements

The requirements for what the notification must contain remain the same as under the existing law. Specifically, the notification must be written in plain language and include, at a minimum, the following information:

- The name and contact information of the reporting person or business
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach
- The following, if it is possible to determine this information at the time the notice is provided:
    - The date of the breach
    - The estimated date of the breach
    - The date range within which the breach occurred
- Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided
- 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

The security breach notification may also include information about what the person or business has done to protect consumers whose information has been breached or advice on steps that the consumers whose information has been breached may take to protect themselves. If a notification must be given to more than 500 California residents as a result of a single breach, the reporting person or business must submit a sample copy of the notification to the state Attorney General.

Implications

The expanded law applies to all agencies, people, and businesses that conduct business in California and that own or license computerized data that includes personal information, as defined in the statute, and requires that security breach notifications must be made to residents of California. California is one of 49 states that have enacted a variety of laws addressing security breach notifications when personally identifiable information is potentially compromised. Individuals and companies should be thoughtful about their collection of personally identifiable information, maintain such information in a secure and encrypted manner to the extent possible, and implement policies to address security breaches in a timely and lawful manner in the event that they occur.

National Law Review, Volume III, Number 284