Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - California

Cal. Civ. Code § 1798.29; **1798.82** ***et seq.***

S.B. 1386 (signed into law September 25, 2002)

Effective July 1, 2003

S.B. 24 (signed into law August 31, 2011)

Effective January 1, 2012

S.B. 46 (signed into law September 27, 2013)

Effective January 1, 2014

AB-1710 (signed into law September 30, 2014)

Effective January 1, 2015

A.B. 964, S.B. 570, S.B. 34 (signed into law October 6, 2015)

Effective January 1, 2016

A.B. 1130 (signed into law on October 11, 2019)

Effective January 1, 2020

Application. Any person, business, or state agency (collectively, Entity) that does business in CA and owns or licenses computerized data that contains PI.

Security Breach Definition. An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification to any CA resident (1) whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person, or (2) whose encrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the Entity that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that PI readable or useable.

Attorney General Notification. If an Entity is required to notify more than 500 CA residents, the Entity shall electronically submit a single sample copy of the notification, excluding any personally identifiable information, to the Attorney General.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own, the Entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition.

1. 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 (meaning rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security):

- Social Security number;
- Driver's license number or state identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
- Account number, credit card number, 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 (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional);
- Health insurance information (an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records);
- Information or data collected through the use or operation of an automated license plate recognition system (a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data); or
- biometric data generated from measurements or technical analysis of human body characteristics (e.g., fingerprint, retina, or iris image) used to authenticate a specific individual.
- Genetic data (data that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material)

2. Username or email address, in combination with a password or security question and answer that would permit access to an online account.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required.

Generally. Notice may be provided by one of the following methods:

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act)

The notice shall be written in plain language and shall include a description of the following:

- The date of the notice;
- Name and contact information of the reporting person or Entity;
- Type of PI subject to the unauthorized access and acquisition;
- The date, estimated date, or date range during which the breach occurred, if it can be determined;
- Whether notification was delayed as a result of law enforcement investigation, if that can be determined;
- 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 state identification card number.

See below re credit monitoring information, if offered. At the Entity's discretion, the notice may also include:

- Information about what the Entity has done to protect individuals whose information has been breached; and
- Advice on steps that the person whose information was breached may take to protect him or herself.

The notice shall be titled "Notice of Data Breach," and shall provide the information above under the headings:

- "What Happened,"
- "What Information Was Involved,"
- "What We Are Doing,"
- "What You Can Do," and
- "More Information."

The notice shall be formatted to call attention to the nature and significance of the information it contains, shall clearly and conspicuously display the title and headings, and shall not contain text smaller than 10-point type. (A model security breach notification form is provided in the statute.)

For online account credentials: Notice may be provided in electronic or other form and should direct CA residents to:

- Promptly change their password, security question or answer, or
- Take other appropriate steps to protect the online account with the Entity and all other online accounts with the same username or email address and password or security question or answer.

For email account credentials: For breaches of login credentials for an email account furnished by the Entity, notice may not be provided to the breached email address, but may be provided via methods otherwise permitted, or via clear and conspicuous notice delivered to the CA resident online when the CA resident is connected to the online account from an IP address or online location from which the Entity knows the CA resident customarily accesses the account.

Credit Monitoring Services. If the person or business offers credit monitoring or identity theft prevention and mitigation services, the services must be provided at no cost to the affected person for not less than 12 months, and all information necessary to take advantage of the offer must be provided in the notice. This provision applies only if the person providing notice was the source of the breach and if the breach exposed or may have exposed PI involving Social Security numbers or covered forms of government identification (driver's license, state identification card numbers, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a

specific individual).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has email addresses for the subject persons;
- Conspicuous posting for at least 30 days of the notice on the Entity's website, if the Entity maintains one (meaning providing a link to the notice on the home page or first significant page after entering the website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link); and
- Notification to major statewide media. State agencies using substitute notice must also notify the California Office of Information Security within the Department of Technology.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of the statute shall be deemed in compliance with the notification requirements of the statute if it notifies subject persons in accordance with its policies.

Exception: HIPAA-Covered Entities. A covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will be deemed to have complied with the individual notice content requirements in this state law if it has complied with the individual notice content requirements in Section 13402(f) of the Health Information Technology for Economic and Clinical Health Act (HITECH). Covered entities are not otherwise exempt from the statute's requirements.

Other Key Provisions:

- **Delay for Law Enforcement.** Notification may be delayed if the law enforcement agency determines that the notification will impede a criminal investigation. The notification required by the statute shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.
- **Private Right of Action.** Any customer injured by a violation of this title may institute a civil action to recover damages. In addition, any business that violates, proposes to violate, or has violated this title may be enjoined.
- Waiver Not Permitted.