JONES DAY

SEPTEMBER 2008

CALIFORNIA EXPANDS SECURITY BREACH NOTIFICATION LAW TO INCLUDE MEDICAL AND HEALTH INSURANCE INFORMATION

The landmark California Database Security Breach Notification Act (the "Notification Law") was amended this year by Assembly Bill 1298 (effective January 1, 2008) to include medical and health insurance information—a change that expands the reach of the law and potential scope of liability and should prompt businesses to revisit their data security policies. The amendment redefines the types of "personal information" whose breach requires a notification to include medical and health insurance information, each of which are construed broadly. As a result, many businesses that may not have maintained personal information that would cause them to come under the ambit of the notification requirements before now may be subject to the law (*e.g.*, employers whose records contain their employees' health insurance information), and certain health care businesses (*e.g.*, hospitals and other health care providers) may now need to comply not only with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") but also will need to comply with the Notification Law. This *Commentary* describes the change in the Notification Law and suggests compliance strategies.

CALIFORNIA DATABASE SECURITY BREACH NOTIFICATION ACT (NOTIFICATION LAW)

The Notification Law (Cal. Civ. Code 1798.29), effective July 2003, requires any person or company conducting business in California that owns, licenses, or stores certain types of computerized personal information to disclose any breach of the security of the system by notifying California residents whose information was, or is reasonably believed to have been, accessed by an unauthorized person. A "breach of the security of the system" is unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. The law applies only to *unencrypted* computerized data. Moreover, the

"personal information" it protects does not include information that is publicly available from legal sources. The prescribed notification methods remain unchanged and are detailed in the Notification Requirements section below. Further details on the original Notification Law are described in a previous *Jones Day Commentary* on the subject ("California Raises the Bar on Data Security and Privacy," September 2003).

Since the Notification Law applies not only to businesses that own or license computerized data, but also to those that simply maintain computerized data that includes California residents' personal information, a broad array of businesses fall under its ambit and must comply with the notification requirements.

MEDICAL AND HEALTH INSURANCE INFORMATION NOW INCLUDED; MORE BREACHES WILL TRIGGER NOTIFICATION OBLIGATIONS

The newly amended definition of "personal information" further extends the Notification Law's reach. Prior to the amendment, the types of unencrypted "personal information" whose breach mandated notification were an individual's first name or first initial and last name in combination with one or more of the following three data elements: (1) Social Security number; (2) driver's license number or California ID card number; or (3) 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. Under the amended Notification Law, medical information and health insurance information have been added to these data elements. Medical information is "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 is "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" (Cal. Civ. Code 1798.29(e)(4) and (5)).

The addition of these two data elements to the types of personal information whose breach can trigger notification obligations means many more security breaches will trigger obligations under the Notification Law. As a result, companies doing business in California should scrutinize the unencrypted computerized data they own, license, or maintain to determine whether it is personal information under the Notification Law. For example, any business that retains unencrypted records of its employees' medical and health insurance histories, or has elements thereof in combination with other unencrypted personal information, should be prepared to comply with the Notification Law in the event of a security breach. Such personal information could be found among Family Medical Leave Act, workers' compensation, and health insurance enrollment records.

Similarly, the addition of medical information and health insurance information to the definition of personal information will affect many health care companies. Prior to the amendment, some health care companies had been able to avoid the Notification Law's obligations by encrypting any Social Security numbers that were maintained electronically. It may be impractical for these companies to similarly encrypt all computerized medical information or health insurance information. Since HIPAA does not mandate security breach notification, hospitals, physicians, and other health care entities covered by HIPAA likely will need to augment their security procedures to be prepared to comply with the Notification Law.

NOTIFICATION REQUIREMENTS

Upon discovery or reasonable belief that a security breach involving personal information has occurred, a company must notify all affected California residents as expediently as possible and without unreasonable delay. If the company owns or licenses the data, the notification may be delayed long enough to take "any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." If the company merely *maintains* the data (and does not own it), then it must notify the owner or licensee of the data immediately following discovery, if the

data was, or is reasonably believed to have been, acquired by an unauthorized person. In both cases, however, notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

Although the Notification Law does not delineate what content must be in the notification, it does prescribe a few specific methods. First, companies may adhere to their own information security notification procedures if those procedures comport with the timing requirements of the Notification Law (Cal. Civ. Code 1798.29(h)). If a company does not maintain its own notification procedure, then it may provide notice either:

- In writing; or
- By electronic notice (if such notice is consistent with USC Title 15, Section 7001, regarding electronic records and signatures); or
- By substitute notice, if the cost of providing the other forms of notice would exceed $250,000, or if more than 500,000 people are affected, or if the company does not have sufficient contact information to fulfill the other types of notice.

Substitute notice consists of more public methods of notification. Companies giving substitute notice must do *all* of the following: (1) provide email notification to the affected California residents if the company has their email addresses; (2) conspicuously post the notice on the company's web site; and (3) notify major statewide media.

STRATEGIES FOR AVOIDING SECURITY BREACHES

Companies that own, license, or maintain unencrypted personal information should take a number of steps to avoid security breaches. First, they should review their policies and practices to ensure that they are adequate for protecting the privacy and security of personal information. They should inventory their computer systems and storage media to identify those containing personal information and should use technologies to identify potential security gaps. Personal information can be classified according to sensitivity, and physical and technological security safeguards can be established to protect the more sensitive information. For example, companies should establish policies that provide employees with access to only the personal information their job responsibilities require, use technological means to restrict access to specific categories of personal information, monitor employee access to sensitive personal information, and remove access privileges of transferred or departed employees immediately.

Companies should promote awareness of security and privacy policies through ongoing employee training and communications. They should also require third-party service providers and business partners that handle personal information on behalf of the company to follow specified security procedures. This can be accomplished by making privacy and security obligations of third parties enforceable by contract, ideally accompanied by indemnification for damages caused by the third parties' breach. Internally, companies should consider employing the use of intrusion-detection technology to ensure rapid detection of unauthorized access to higher-risk personal information and, wherever feasible, use data encryption, in combination with host protection and access control, to protect sensitive information. Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard. Companies should also dispose of records and equipment containing personal information in a secure manner, such as shredding paper records and using a program to "wipe" and overwrite the data on hard drives.

Companies should also be prepared to comply with the Notification Law in the event of a security breach by implementing measures such as determining the contact information for, and the best means of notifying, the affected individuals in the event of a security breach involving personal information. They should develop internal assessment procedures and contingency plans for investigating the scope and source of a security breach, possibly with the assistance of outside investigators, and for taking corrective actions to remediate harm and prevent further breaches. Finally, they should develop a contingency public relations plan to minimize damage to the company's reputation resulting from a security breach.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Kevin D. Lyles
1.614.281.3821
kdlyles@jonesday.com

Jeffrey M. Rawitz
1.213.243.2537
jrawitz@jonesday.com

This Commentary *was prepared with the assistance of Shira Kelber, a summer associate in the San Francisco Office.*