california requires disclosure of database security breaches

by Dan Appelman

Dan Appelman is a partner in the international law firm of Heller Ehrman, White & McAuliffe, LLP. He practices intellectual property and commercial law, primarily with technology clients, and is the current chair of the California Bar Association's Standing Committee on Cyberspace Law.

dan@hewm.com

A new California law took effect on July 1, 2003 which requires businesses to disclose to California residents any breach in the security of their computerized data when that breach results in the acquisition of personal information about those California residents by unauthorized users. California Civil Code Section 1798.82 also requires businesses maintaining computerized data for others to notify the owners of that data should it be acquired by an unauthorized user.

Approved by former Governor Gray Davis in 2002, the law has sweeping implications for a wide range of businesses located both inside and outside of California. Experts estimate that nearly 100,000 security breaches occur every year.[1] Many of these breaches affect California residents. Companies that encrypt all personal data in their databases are exempt from the new law's disclosure requirements. Those that do not must fully comply with the new law, as the penalties for its violation include both monetary damages and injunctive relief.

The New Law

California Civil Code Section 1798.82 provides: "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The law also provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The notification requirements apply to any disclosure of "personal information." In order to be considered "personal information" under the new law, the information stored must include information from each of two categories. The first, or "name" category, is the California resident's first name or initial and last name. The second, or "information" portion, is either a social security number, a driver's license number, a California identification card number, or a credit or debit card account number plus any related information necessary to utilize the account.[2]

Businesses are required to notify California residents of any breach in "the most expedient time possible and without unreasonable delay." Businesses may meet this requirement with a written notice, or they may send an electronic notice,[3] provided that they receive an individual's valid consent to electronic notification.[4]

1. "California Sleeper" *Daily Deal*, April 7, 2003.

2. Information made public by local, state, or federal governments does not constitute personal information for purposes of the new law.

3. The new law provides that disclosure by electronic notice is permissible if it complies with the provisions regarding electronic records and signatures set forth in the federal law known as the Electronic Signatures in Global and National Commerce Act (15 USC § 7001 et seq.).

4. If a law enforcement agency believes that the notification would hinder an investigation, it can waive the notice requirement for a period of time.

A business whose notification is targeted at more than half a million people or would cost in excess of $250,000 is eligible to make a different type of notification. In that case, the law requires the use of email notification,[5] conspicuous posting on the company's Web site, and notification of the statewide media.

What Type of Breach Requires Notification

Requiring public notification of security breaches will be a sensitive matter for most companies. It is therefore important to understand the law, how it is implemented and enforced, and how to comply with it.

The legislature made clear that this is an act targeted primarily at reducing exposure to identity theft. According to its proponents, the notification required by the new law will provide the victims of identity theft with more time to mitigate the damages that can result from an unauthorized acquisition of their personal information.

However, the statute only vaguely defines what type of security breach triggers the notification requirement. The statute defines a "breach of the security of the system" as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." The business's duty to notify California residents is triggered upon the discovery of the breach.

Note that the statute requires notification based not only on the event of compromised "confidentiality," but also when "security" or "integrity" is compromised. Courts may give independent meaning to the terms "security" and "integrity," or they may view the whole phrase as a term of art.[6]

Importantly, the law does not require notification when either the name portion or the information portion of the personal information has been encrypted. But businesses seeking to take advantage of this may be surprised to find that the statute does not define what standard of encryption is sufficient to exempt them from the notification requirement.

Also, the statute does not require notification if the unauthorized person who acquires a California resident's personal information is an agent or employee of the information-owning business, the acquisition was in good faith, and the information is not further disclosed.

Extra-Territorial Application of Section 1798.82

The new law applies to a company if it conducts business in California. The law leaves to the courts the determination, on a case-by-case basis, of whether a given company located outside of California is conducting sufficient business in California that the notification and disclosure requirements will apply. The lack of guidance in the statute makes it impossible for a company to know in advance whether it must comply with the California law.

The jurisdiction of the California courts extends as far as allowed under the Due Process clause of the federal Constitution. It is clear that California courts have jurisdiction over all companies whose principal place of business or headquarters is located in California. Likewise, California courts have jurisdiction over companies located outside of California whose contacts within California are "systematic" and "continuous" enough that the defendant might anticipate litigating any claim in the state.

5. The new law intentionally uses the term "electronic notice" in one section and "e-mail notice" in another. To be effective and compliant, "electronic notices" must comply with the Electronic Signatures in Global and National Commerce Act, whereas "e-mail notices" (as part of the substitute notice provisions) apparently need not.

6. Furthermore, in its original form, Section 1798.82 stated that mere unauthorized access would constitute a breach that would trigger the notice and disclosure requirements. Amended before passage, the statute now provides that unauthorized acquisition, not access, triggers the requirements. It will be up to courts to decide whether there is a significant difference between these two terms.

The new law also applies to companies located elsewhere that engage in even minimum marketing or sales transactions with California residents.

However, jurisdiction generally does not apply to businesses that have no property in California, that have not sought to enter the California marketplace, and that have no telephone listings in California or any other contacts with California.

Companies headquartered and maintaining their principal places of business outside of California, but having business relations with California, may or may not be subject to California's jurisdiction for purposes of enforcing their compliance with the new law. The inquiry is a fact-intensive one. Courts look to whether the company "purposefully availed" itself by directing its actions at the state, so that it enjoys the benefits and protections of the state's laws. The claim must arise out of the company's actions that are directed at the state, and the jurisdiction must comport with the interests of "fair play and substantial justice."

Typically, the requirement that a company purposefully avail itself is met by demonstrating that it conducts continuing business relationships with citizens of the state. Even a single contact may be enough, depending on the nature and consequences of the contacts. Moreover, courts generally view a company's contacts as cumulative, so minimal contacts over a period of time may bring the company within the jurisdiction of California law and the California courts.

Internet Contacts

It is difficult to predict how a company's contacts will be viewed when those contacts with California are solely via the Internet. Internet Web pages are viewable anywhere, and while the Internet allows buyers to choose among more sellers, it is difficult for a seller to define where its customers come from. Courts tend to look at the nature of the contact and how the Internet Web page functions. The more interactive an Internet Web page, the more compelling the basis for asserting jurisdiction over those responsible for it. Other important factors include whether the initial contact is directed to the buyer (as in directed email) or is merely a passive advertisement.

Conclusion

It is likely that the new law will have a material impact on all companies that maintain data about California residents in their computerized databases. Companies that have offices, assets, or employees in California certainly have to comply with the new notification and disclosure requirements. But the new law also applies to companies located elsewhere that engage in even minimum marketing or sales transactions with California residents.

Despite the many uncertainties surrounding the new law, businesses should plan conservatively in order to comply with the fair meaning of the statute. This means that businesses should consider either immediately encrypting computerized personal information or develop strategies in order to meet their statutory notification requirements in the event of a security breach. Businesses may also want to take steps to decrease their potential costs of complying with the new law's notification requirements by adjusting their current intake forms to include a provision where the customer can consent to electronic notification in the event of a security breach.