NEWMEYER & DILLION LLP

Understanding California's Data Breach Notification Law: Protecting your Company & Customers

By: Brandy L. Worden

The California Attorney General's 2016 Data Breach Report found 3 out of 5 Californians were victims of data breaches and that data breach victims were significantly more likely to experience identity theft. Notifying consumers of a data breach promptly after it happens allows and encourages them to take proactive measures (such as cancelling susceptible credit cards, purchasing identity theft prevention services, and so forth) to prevent identity theft. When consumers affirmatively act to prevent identity theft, they also minimize the amount of damages they might otherwise have that your company may ultimately be liable for.

California has been a trailblazer in the field of data breach transparency. In 2002, California became the first state to enact its Data Breach Notification Law. This law has become a model that has been followed by many states across the United States. The law has been tweaked over the years, with new amendments having gone into effect as recently as January 2017.

Here's an overview of some key provisions of the law to help your company comply with the law and reduce its exposure when confidential data is breached:

When is Notice Required

Under the California Data Breach Notification Law (Civil Code section 1798.82) you are required to provide notice of a data breach if:

1. You are doing business in California;
2. You own or license computerized data;
3. The data includes personal information of clients residing in California;
4. There was an unauthorized acquisition of electronic personal data of California residents; and
5. The personal data is not encrypted, or it is encrypted but there is reason to believe the encryption key was also compromised.

If more than 500 California residents are impacted by the breach, the California Attorney General's Office must be notified electronically by submitting to it a single sample copy of the notice, excluding any personally identifiable information.

What is "Personal Information"

The law defines personal information as an individual's first name or first initial and last name in combination with any one or more of the following:

1. Social security number;
2. Driver's license/ID card number;
3. Account or card numbers if combined with a security/access code;
4. Medical information;
5. Health insurance information; or
6. Data collected from an automated license plate recognition system.

Personal information is also defined as a user name or email address, in combination with a password or security question and answer that would permit assess to an online account.

Timing for Notice

The California Data Breach Notification Law does not provide a certain number of days, weeks, or months within which you must provide notice. Rather, companies are to provide notice "in the most expedient time possible and without unreasonable delay" and "immediately following discovery." To add to the uncertainty, notice can be delayed to avoid interference with law enforcement investigations or if necessary to determine the scope of the breach and to restore the integrity of the data system.

What to Include in Notice

The law has been amended to make it easier for consumers to understand the notice. The notice must be titled "Notice of Data Breach" and include specific details about the breach under the following headings:

1. "What Happened"
2. "What Information Was Involved"
3. "What We Are Doing"
4. "What Can You Do"
5. "Other Important Information"
6. "For More Information"

Under certain circumstances, if the breach exposed social security numbers, driver's license numbers, or California identification card numbers, then an offer to provide appropriate identity theft prevention and mitigation services must be included in the notice. These services must be provided at no cost to the affected person for not less than 12 months and the notice must contain information necessary to take advantage of the offer.

Despite California's efforts to "simplify" breach notification, California's Data Breach Notification Law is technical and fraught with liability if you do not respond properly. Understanding the law can help protect your customers and your company. We recommend that companies have a data breach response plan in place before a breach occurs that includes the steps needed to comply with the notice requirements.

If your company needs assistance drafting such policies, or has faced a data breach, Newmeyer & Dillion's Cybersecurity Team can help. For assistance reviewing your coverage, please contact managing partner, Jeff Dennis, Esq. based in the Newport Beach office (949.854.7000; jeff.dennis@ndlf.com) or managing partner, Nathan Owens, Esq. of the Las Vegas office (702.777.7500; nathan.owens@ndlf.com).

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.