

Daily Journal

JANUARY 21, 2015

NEW CALIFORNIA LAWS

FOR 2015

AB 1710: New rules for managing data breaches

By Mark D. Selwyn and Leizel Ching

In 2013, 167 data breaches — affecting millions of Californians — were reported. While breaches affected many industries, the vast majority stemmed from breaches reported by the retail industry. In response, the Assembly Judiciary and Banking and Finance Committees held a hearing to examine whether California law should be updated. Assembly Bill 1710, born out of this hearing, was signed into law Sept. 30, 2014.

The most discussed part of the new law is a subsection stating, “If the person or business providing the notification [of the data breach] was the source of the breach [of Social Security numbers or driver’s license numbers], an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months.” The “if any” language has generated some confusion as to whether the law imposes a mandatory requirement that businesses provide

12 months of services or whether the law only requires businesses that elect to provide such services to do so free of charge for 12 months. Attorney General Kamala Harris, in her 2014 Data Breach Report, interprets the new law as instituting a mandatory requirement.

The phrase “source of the breach” is undefined. This may lead to disputes between companies and third-party vendors, e.g., cloud service providers, regarding who is responsible in the event of a data breach.

The prevention and mitigation services requirement is not triggered by breaches of payment card data or online credentials (the vast majority), only those involving Social Security and driver’s license numbers. The latter breaches expose victims to one of the most serious types of identity theft, new account fraud.

While data “owners” must notify affected individuals of a breach “in the most expedient time possible and without unreasonable delay,” data “maintainers” must notify the “owners” or “licensees” “imme-

diately following discovery” of a breach. While “owners” and “maintainers” are undefined, Section 1798.81.5(a)(2) defines what it means for a business to “own” and “maintain” personal information. Courts may use these definitions as the bases from which to interpret whether a business is a data “owner” or “maintainer.”

AB 1710 is effective as of Jan. 1, 2015. Companies should review and update their privacy and security policies to ensure compliance. Companies should provide training to all who handle personal information. Violators could face damages and injunctive relief.

Mark D. Selwyn is a partner in WilmerHale’s Palo Alto office, co-chair of the Intellectual Property Litigation Practice Group and a member of the firm’s Management Committee and its Litigation/Controversy Department. You can reach him at Mark.Selwyn@wilmerhale.com.

Leizel Ching is a senior associate in the firm’s Palo Alto office. You can reach her at Leizel.Ching@wilmerhale.com.