crowell moring

CLIENT ALERT

California Enacts Tough New Privacy Protections

Oct.02.2014

On September 30, 2014, California Governor Jerry Brown signed into law Assembly Bill 1710, which contains a new set of personal information protections that affect all businesses that "own, license, or maintain personal information about Californians." In what may become a precedent for other jurisdictions, the law includes the nation's first mandatory state requirement for breached entities to offer breach mitigation services – including credit monitoring – to all affected individuals. Further, the law includes new restrictions on the sale of social security numbers (SSNs). These amendments to the existing California Civil Code Sections 1798.81.5, 1798.82, and 1798.85 will take effect on January 1, 2015.

While offering some sort of breach mitigation services has become common practice for breached entities, California will now require any notifying entity that is the source of a breach to "offer to provide appropriate identity theft prevention and mitigation services … at no cost to the affected person for not less than 12 months." This obligation will apply only to breaches involving Californians' names combined with an SSN, driver's license number, or California ID number.

California has also expanded the scope of its pre-breach privacy protections by including, in addition to business that "own or license" personal information about California residents, businesses that simply "maintain" such information. Now "a business that owns, licenses, or maintains personal information about a California resident" is required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure." This could have a significant impact on service providers tasked with maintaining covered information.

Finally, the new law limits the sale of social security numbers. While carving out an exception for "release of an individual's social security number if the release … is incidental to a larger transaction," the law states that businesses may not "sell, advertise for sale, or offer to sell an individual's social security number."

The bill that passed left out some of the more stringent provisions included in an earlier proposal. Based on industry comments, the bill's co-sponsors removed provisions that included limits on the amount of payment information a retailer could store in its system as well as more stringent encryption standards. Nevertheless, this new law will affect a broad range

Recent Happenings in APRM
October 2014

- When Internet Connectivity Features Fail – is the Product Unsafe, or Just Not "Smart"?
- The European Commission Issues a "Myth-Busting" Factsheet to Address the Concerns That Have Emerged After the EU Court of Justice's Ruling On Search Engines and the "Right to Be Forgotten"
- Think of the Children: Guidelines for Advertising Food and Alcohol
- Proposition 65 – Warning Regulation Update
- Why You Should Comment on the CPSC Certificate of Compliance Filings at Entry
- California Enacts Tough New Privacy Protections
- FDA Publishes Cyber Guidance for Medical Devices
- To Label Or Not To Label? Companies May Have No Choice

of businesses and anyone else who "maintains" the personal information of California residents, and those businesses should review the new requirements carefully to understand their compliance requirements.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com