BY NEAL SALISIAN AND KATHARINE MINER

New Consumer Data Protections Increase Liability Risk

CALIFORNIA IS A LEADER IN consumer protection legislation, and in the wake of recent high-profile data breaches, the legislature enacted AB 1710, which was signed into law by Governor Jerry Brown and took effect on January 1, amending Sections 1798.81.5, 1798.82, and 1798.85 of the Civil Code.

Businesses that deal with consumers should be aware that AB1710 restricts disclosure of Social Security numbers and mandates identity theft monitoring protections. Businesses in California must take note, as their consumer data policies and procedures may no longer be in compliance. There are at three least noteworthy changes.

The first change is an expanded application of security procedure requirements. The new law increases the number of businesses required to implement security procedures. Previously, only businesses that owned or licensed a consumer's personal information were 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." AB1710 significantly expands the application of these requirements to businesses that maintain personal information. "Personal" is defined as an individual's first name or first initial and last name, in combination with a Social Security number, driver's license number, medical information, or certain financial account information, when at least some of that information is not encrypted or redacted.

Businesses that own or license personal information are defined under the law as those that retain the information as part of their internal customer accounts or for the purpose of using that information in transaction with the person to whom the information relates. The law is less explicit in defining when a business "maintains" personal information, stating only that "the term 'maintain' includes personal information that a business maintains but does not own or license."

Notification and Creditor Monitoring

In the event of a breach, California's privacy laws require businesses to follow certain notification requirements. Specifically, businesses that own or license data must notify consumers whose information was or "is reasonably believed to have been acquired by an unauthorized person...in the most expedient time without delay," while businesses that maintain personal information must immediately notify the owner or licensee of the data of the breach.

As an additional change, AB1710 increases the corporate obligation by requiring free credit monitoring services in some cases of breach. If a business was the source of the breach and the breach involves an individual's name and Social Security number, driver's license number, or California identification card number, "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 ambiguous "if any" language has spawned debate regarding the scope and application of this creditor monitoring provision. Some read the provision to require all businesses that are the source of the breach to offer no-cost credit monitoring for at least one year while others argue that only businesses already offering such services will be required to comply. Further complicating matters, the law provides no clarity on what constitutes "appropriate identity theft and mitigation services." Until the California courts consider this question, or the Attorney General sheds some light on the breadth of this provision, businesses must be prepared to provide credit monitoring services.

AB1710 increases the corporate obligation by requiring free credit monitoring services in some cases of breach.

And the services must be offered for free and for no less than one year. While this may not be a significant change for many larger corporations that provide credit-monitoring services as a matter of practice, it is the smaller businesses that are likely to be most affected by these additional requirements and the uncertainty of their application.

Lastly, AB1710 also restricts disclosures of Social Security numbers, prohibiting the sale, advertisement for sale, or offer to sell an individual's Social Security number. Exceptions apply if the release of a Social Security number is incidental to a larger business transaction, and the release is necessary to identify the individual in order to accomplish a legitimate business purpose. But the law is clear that the release of Social Security numbers for marketing purposes remains unpermitted.

AB 1710 is undoubtedly a significant expansion of California's consumer data protections. But it remains to be seen how broadly these protections will be interpreted. Until further guidance is provided, the ambiguous drafting of the identity theft monitoring provisions, in particular, will pose difficulties for businesses trying to structure code-complaint breach procedures. If data breaches are not perilous enough, now navigating the legal implications of them could prove equally disconcerting. It will also be worth watching whether other states follow in California's footsteps and enact similar legislation, or if the federal government will step in to address the diverse state approaches to consumer privacy protection.

Until that time, businesses will need to stay current with the laws of each state where they do business. State regulations will likely continue the trend toward greater data security regulation. This means businesses that handle consumers' personal information will need to budget and plan for increased costs and liability. ■

Neal Salisian is a partner, and Katharine Miner a former associate, with Salisian Lee LLP in Los Angeles.