Proskauer

Data Breaches and Damages: Consumer Action Under the CCPA

Minding Your Business Blog on **December 2, 2019**

With less than one month to go before the California Consumer Privacy Act of 2018's ("CCPA") effective date of January 1, 2020, businesses should be aware of the potential litigation that awaits them.

The CCPA is a California privacy law that gives California consumers the rights to know about and control the personal information that businesses collect about them. In turn, the CCPA requires businesses to give consumers the ability to effectuate these rights. For a more in-depth review of the CCPA, please view our previous posts on our Privacy Law Blog.

Among the rights the CCPA endows on California consumers, is the right to bring an action for statutory damages if the consumer's information is subject to a data breach. This right, however, only applies to certain kinds of data breaches.

In order for a data breach to be actionable, three requirements must be met:

First, the information must be personal information, not as broadly defined by the CCPA, but as narrowly defined by California's data breach notification law. This is welcome news to breached entities who are wary of consumer actions.

The CCPA's broad definition of "personal information," which would apply to virtually every other part of the Act, is any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." By contrast, the much narrower definition applicable to the data breach notification law lists specific types of information that qualify as personal information, such as a first name or initial combined with social security number.

Second, the personal information must be nonencrypted *and* nonredacted. Note that the requirement that the information be both nonencrypted and nonredacted is a new requirement. The CCPA as enacted in 2018 only required that the information be either nonencrypted *or* nonredacted. A recent amendment changed "nonencrypted *or* nonredacted" to "nonencrypted *and* nonredacted," thus narrowing the consumer's right of action with but a single word.

Third, the breach must have been "a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."

The exact contours of "reasonable security procedures and practices" is yet to be defined for CCPA purposes—neither the text of the CCPA nor Attorney General Xavier Becerra's proposed implementing regulations define "reasonable security procedures and practices." But, entities are not without any guidance: "reasonable security" is not a new standard and is used in other laws such as California's information security statute and the federal Graham-Leach-Bliley Act. In contemplating what "reasonable security" means in those contexts, in 2016, then California Attorney General Kamala Harris released the 2016 Data Breach Report. There, Harris adopted the Center for Internet Security's list of 20 Critical Security Controls to "define a minimum level of information security that all organizations that collect or maintain personal information should meet." Harris's recommendation, which, though not binding is instructive, was that a "failure to implement all the Controls that apply to an organization's environment *constitutes a lack of reasonable security*." (emphasis added).

A deep dive into the Controls is beyond the scope of this post, but the controls can be divided into 3 broad categories: Basic Controls (e.g., "Inventory and Control of Hardware Assets"); Foundational Controls (e.g., "Malware Defenses"); and Organizational Controls (e.g., "Incident Response and Management"). More information on the Security Controls can be found on the Center for Internet Security's website (available here).

If a consumer meets the above three requirements, they are potentially eligible to bring an action for statutory damages on either an individual or class-wide basis. Before bringing the action, the consumer must provide the business with 30 days' written notice, identifying the specific provisions the consumer alleges the business violated. If the business cures the violation, the consumer may only bring an action for pecuniary damages. If the business does not, the consumer may initiate a civil action for:

- Monetary damages of $100-$750 per consumer per incident or actual damages, whichever is greater.
- Injunctive relief or declaratory relief
- Any other relief the court deems proper.

Note that the consumer need not show actual damages to bring a statutory action—they only need to show that their personal, nonredacted and nonencrypted personal information was subject to a qualifying data breach.

Consumers may begin bringing actions on the CCPA's effective date of January 1, 2020. Although other provisions of the CCPA have a 12-month look back period, there is no such language in the data breach provision. Consumers, therefore, will likely only be able to bring actions for data breaches occurring on or after January 1, 2020.

For more insights or inquiries on the CCPA, please reach out to your Proskauer lawyers: Ryan Blaney, Lary Alan Rappaport, Christina Kroll or Divya Taneja.

View Original

Related Professionals

- **Christina Kroll**
  Associate