# Key Provisions of California's Data Breach Law Have Yet To Be Determined

Skadden

06 / 28 / 21

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

**William Ridgway**
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

**Leena El-Sadek**
Associate / Chicago
312.407.0109
leena.el-sadek@skadden.com



One Manhattan West
New York, NY 10001
212.735.3000

155 N. Wacker Drive
Chicago, IL 60606
312.407.0700

In the second year of litigation under the California Consumer Protection Act, a flood of cases continues unabated. When businesses subject to the CCPA experience a data breach, they routinely face consumer class actions seeking the act's steep statutory damages. As these cases wind their way through the courts, one key unresolved issue is how businesses can avail themselves of the CCPA's "notice and cure" provision to avoid these damages.

## Who's Impacted

The CCPA applies to any business that engages with California consumers for profits and:

- has annual gross revenue of at least $25 million;
- buys, receives or sells the personal information of at least 50,000 consumers; or
- derives at least 50% of its revenues from selling consumers' personal information.

Even businesses not directly subject to the CCPA should monitor how the act is enforced. While California was the first state to enact strong data protection laws for its residents, others will surely follow. Several states, such as Washington, New York and Nebraska, have already drafted similar privacy bills to enhance security for their consumers' data. The CCPA, and particularly its private enforcement model, will likely become a blueprint for other states.

## A Private Right of Action To Enforce 'Reasonable Security'

The CCPA's private right of action allows consumers, as individuals or a class, to sue businesses when their personal information is disclosed without their authorization. To recover monetary damages, the consumer must prove the business failed to "maintain reasonable security procedures and practices."

The CCPA does not define "reasonable security procedures and practices," but businesses can look to the 2016 California Data Breach Report published by the California Attorney General for guidance. The report lists five recommendations for organizations to reduce the risk of data breaches and mitigate the resulting harms:

- Implement the Center for Internet Security's recommended controls;
- Use multifactor authentication on consumer-facing online accounts;
- Exercise strong encryption to protect information;
- Encourage individuals to file a fraud alert on their credit files; and
- Urge state policy makers to harmonize state breach laws.

## Notice and Cure Provision

The CCPA's notice and cure provision may provide businesses a way to avoid statutory damages, which, at $150 to $750 per individual, can add up to a daunting figure in a class action. Yet, after more than 18 months of CCPA lawsuits, the contours of the cure defense remain undefined, as early case law has not interpreted which violations are capable of being "cured" and how.

**How the notice and cure provision operates:** A consumer planning to file a suit seeking statutory damages must give the business 30 days advance written notice. If the plaintiff does not notify the alleged violator before filing, the action may be subject to dismissal.

# Key Provisions of California's Data Breach Law Have Yet To Be Determined

After receiving a notice of its alleged violation, a business may cure it within 30 days and provide the plaintiff a written notice of the cure and a guarantee that no other violation will occur in the future. Completing these steps protects a business from statutory damages under the act.

Businesses must carefully assess how to respond to notices of alleged violations. While the possibility of avoiding statutory damages is ample incentive to respond with a cure and guarantee, businesses should consult with attorneys to consider whether plaintiffs may later use modifications of security practices or written guarantees as proof the businesses violated the act in t he first place.

**What constitutes a cure?** Neither the CCPA nor subsequent court decisions have clarified what qualifies as a proper cure. The primary debate centers on whether a cure should aim to (a) remedy a business's deficient security protocols to ensure future compliance with the act or (b) make victims of a data breach whole and prevent continued harm from the breach.

The CCPA's language suggests that certain violations cannot be cured at all, and that the cure provision applies "[i]n the event a cure is possible." Taking note of this language, plaintiffs may attempt to bypass the notice and cure requirements by arguing that the alleged violation is uncurable. Whether courts will allow plaintiffs to take this position remains unclear.

## Takeaways

- Given the volume of CCPA litigation, businesses across the country should watch trends in California and prepare to see similar legislation in other states.
- Businesses that receive a CCPA violation notice must carefully consider the pros and cons of attempting to cure the alleged violation, and the manner in which they characterize any cure.
- While the CCPA's cure provision may be a viable defense in some situations, companies cannot depend on this unclear, after-the-fact solution. They should proactively ensure compliance with best cybersecurity practices before any violations are alleged.