Bloomberg Law

Professional Perspective

Navigating the CCPA's 'Notice and Cure' Provision

James M. Perez and Sheri Porath Rockwell, Sidley Austin LLP

Navigating the CCPA's 'Notice and Cure' Provision

Contributed by James M. Perez and Sheri Porath Rockwell, Sidley Austin LLP

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm.

Companies doing business with California consumers are impacted by the California Consumer Privacy Act (effective Jan. 1, 2020). The CCPA's private right of action provision gives California residents the right to sue companies when their personal information is subject to unauthorized access and exfiltration, theft, or disclosure due to a company's failure "to implement and maintain reasonable security procedures and practices."

Under this provision, consumers may seek actual damages, declaratory or injunctive relief, and statutory damages, which begin at $100 and continue up to $750 "per consumer per incident." The potential aggregated exposure through consumer class actions could be significant, and companies are searching for ways to mitigate private lawsuits.

The CCPA's 'Notice and Cure' Provision

One promising avenue for companies navigating the CCPA is its "notice and cure" provision. Under that provision, a private plaintiff must provide a business with 30 days' written notice "identifying the specific provisions of this title the consumer alleges have been or are being violated," prior to filing their lawsuit. The provision provides that "[i]n the event a cure is possible," a company can avoid "individual statutory damages or class-wide statutory damages" if it "actually cures" the violations within 30 days and provide the consumer with "an express written statement that the violations have been cured and that no further violations shall occur[.]"

If the company later breaches its written statement, "the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement."

While the notice and cure provision will not affect lawsuits for actual damages, it provides an avenue for companies seeking to avoid consumer class actions for statutory damages. For this reason, it is sure to become one of the most utilized and, by extension, hotly contested parts of the CCPA. Companies therefore need to understand how to navigate the notice and cure provision and be mindful of the provision's opportunities and pitfalls. A few considerations that companies should keep in mind follow.

The Consumer Notice

The CCPA imposes a number of requirements on companies doing business with California consumers. However, there is only one CCPA violation available to private litigants: a "business' violation of the duty to implement and maintain reasonable security procedures and practices," which results in an unauthorized disclosure or theft of personal information. This could be a data breach, or simply an unauthorized or accidental disclosure of personal information.

Upon receiving a written notice to cure from a consumer, a company should first examine whether the notice alleges a company's lack of reasonable security procedures and practices that resulted in the purported loss of personal information. A demand to cure other types of alleged violations of the CCPA would be defective. For example, a defective notice may question the company's alleged failure to stop the sale of personal information after the consumer made such a request, target privacy policies with purportedly inadequate descriptions of the categories of personal information the company shares with third parties, or merely complain of a data breach, without articulating the company's alleged violation of its duty to provide reasonable security measures that may have resulted in the breach.

In the event a consumer serves a defective notice and 30 days later files a lawsuit, a defendant company should consider filing a motion to dismiss based on the consumer's failure to comply with the statute's mandatory pre-suit notice requirement or the consumer's lack of standing to bring the lawsuit in the first place.

Companies may also want to begin laying the groundwork to demonstrate that they do in fact implement "reasonable security practices and procedures," by fortifying their documentation, undergoing a data security audit, or obtaining third-party certifications, for example.

The CCPA provides no guidance about important procedural issues that may arise with notices to cure and may be the subject of CCPA litigation. These include the time limit (if any) within which a consumer must serve a notice to cure after becoming aware of the loss of personal information, whether consumers can conflate the mere fact of a data breach with a violation of the duty to provide reasonable security measures, and whether the consumer must identify specific security measures the company did not take that allegedly resulted in the breach or disclosure.

Assessing What Constitutes a Cure

The notice and cure provision gives companies an opportunity to "cure" their violations within 30 days, but only "[i]n the event a cure is possible[.]" What qualifies as a "cure" for unreasonable information security is not defined in the statute, and the lack of clarity around the cure provision was the subject of several comments submitted during the Attorney General's CCPA "public listening" tour in early 2019.

The AG may provide some guidance on this question in forthcoming regulations. However, because the notice and cure provision is not among the seven specific issues the AG is required to address in its regulations, it is also possible this question will be left to the courts to decide. Because of this uncertainty, and because notices to cure may arrive on companies' doorsteps months before the deadline for the AG's final regulations (July 2020), companies and their counsel should begin evaluating their options.

In the wake of the passage of the CCPA, there has been much speculation about various theories on a "cure" for the loss of personal information due to a data breach, such as free credit monitoring, destruction of data acquired without authorization, or attestations from the improper recipients. However, it is important to emphasize that the cure provision relates to the company's violation of its duty to maintain reasonable information security, which, in turn, led to the purported loss of personal information as a result of the data breach. The cure provision does not relate to curing the loss of personal information itself.

Private plaintiffs nevertheless may argue that "no cure is possible" after the loss of personal information as a result of a company's failure to maintain reasonable security measures—which the plain language of the statute dictates is the only CCPA violation consumers can sue for. Accordingly, they may take the position there is no requirement that they comply with the notice provision at all. This argument would effectively render the entire cure provision obsolete, and runs counter to the well-established principle that courts must give effect to all provisions of a statute, such that no part of the statute will be inoperative or superfluous.

When evaluating how to "actually cure" an alleged violation noticed by a consumer, a company should consider the range of possible responses that, while not placing the "genie back in the bottle," nevertheless enhances its data security. The company may draw from elements of enhanced data security practices included in data breach settlements, FTC consent decrees, or data security best practices and guidance. A commitment to increase data security staff, to engage in periodic data security testing, or to increase amounts spent on data security may be among the factors considered good-faith efforts to "cure" the unreasonable information security practices that may have contributed to a data breach.

The appropriate "cure" will need to be informed by the circumstances of each breach and the affected company's existing security program. Choices will need to be made carefully and deliberately, but also quickly; there is only a 30-day window, and unlike other provisions of the CCPA (e.g., time by which to respond to a verified consumer request for information), the statute does not provide for extensions of time for compliance. Thus, advance consideration is key.

Express Written Statement

Careful consideration should be given to the written statement that a company is required to make certifying both that the violation has been cured and that "no further violations shall occur." These statements should, at the very least, be consistent with other representations that the company has made—or will make—about the data breach and the company's efforts to address ongoing vulnerabilities. They should also be consistent with representations made in privacy policies and consumer-facing descriptions of the company's data security practices.

Key Takeaways

The CCPA's "notice and cure" provision has the potential to provide an effective defense against the CCPA consumer class action lawsuits that will likely follow any data breach after the law takes effect. Yet, the "notice and cure" provision raises more questions than it answers. Companies doing business with California consumers will need to respond carefully when they receive a consumer's notice to cure. Companies should anticipate, and prepare for, consumer efforts to avoid the procedure or aggressively challenge the adequacy of any company response, as consumers will press to take full advantage of the statutory damages available in CCPA private suits.