PAUL HASTINGS

STAY CURRENT

June 2019

Follow @Paul_Hastings

Steps You Can Take Now To Reduce The Risk Of Litigation Under The New California Consumer Privacy Act

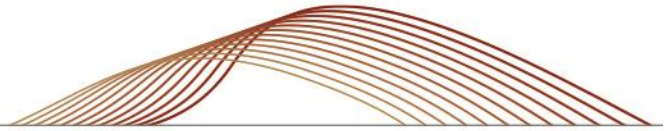
By Robert P. Silvers, Danielle D. Decker, Behnam Dayanim, Sherrese M. Smith & John P. Phillips

The private cause of action for statutory damages created by the California Consumer Privacy Act ("CCPA") will go into effect on January 1, 2020, clearing the way for consumer class actions in the wake of a data breach. This new right will change the status quo for companies doing business in California and significantly increase their potential damages exposure. The law's unique features, including a 30-day notice period and opportunity to cure, make preparation paramount. In this client alert we discuss what the CCPA's new right of action entails, and how companies can take proactive steps to manage the litigation risks that will arrive New Year's Day.

I. The Potential Classwide Statutory Damages Available Under the CCPA Are Huge

Any company that owns, licenses, or maintains personal information about Californians may be subject to the CCPA's private right of action. Given that there are nearly 40 million California residents, millions of companies may be subject to the new law. The CCPA provides that a consumer seeking to sue under the statute must show that his or her unencrypted or nonredacted personal information (as defined by the statute) was accessed and taken as a result of the company's failure to maintain reasonable security procedures. Cal. Civ. Code § 1798.150. The CCPA requires that a successful plaintiff seeking statutory damages recover a minimum of $100, and a maximum of $750 per violation. The potential liability can be staggering: For example, a security incident involving one million California records could lead to the recovery of up to $750 million in statutory damages in a class action (and no less than $100 million if a court sustains a finding of liability). This type of damages award represents a dramatic shift from prior law.

Before the CCPA created a right to statutory damages based on a data breach, a private litigant was required to prove actual damages to bring a claim (unless the violation was willful or reckless). Proving injury was no easy task, and even provable damages were often too insignificant and variable among class members to justify the costs of litigation. As a result, class action litigation related to data breaches often failed at the outset or settled in the early stages. Regulators, in contrast, have long had the authority to pursue substantial statutory penalties for data breach violations, but those enforcement actions are subject to the constraints of government resources, making them few and far between.



The CCPA removes these hurdles and practical impediments to substantial damages for a data breach. Its private right of action for statutory penalties arms every data breach victim with the right to pursue classwide relief. Because plaintiffs will be entitled to statutory damages without having to prove individual harm, class actions will proliferate as the possibility of a significant damages verdict encourages plaintiff attorneys to file suit. For these main reasons, when the CCPA goes into effect on January 1, 2020, companies will face a new and substantial risk of litigation after suffering a data breach, which explains in part why so many companies have been working diligently to tighten compliance programs and critically assess the measures in place to prevent a breach.

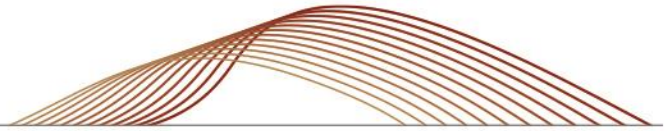
II. The CCPA Gives Companies a Chance to Cure the Violation, and To Disqualify Class Representatives

The CCPA includes a provision that may substantially mitigate companies' liability. Thirty days before initiating suit, the CCPA requires any consumer seeking individual or classwide statutory damages to provide notice to the company of an alleged violation under the statute. If the company cures the violation and provides the consumer with a written statement that the violation has been cured, and that no further violations shall occur, the consumer is barred from bringing an action for individual or classwide statutory damages. The concept of a statutory cure period following a data breach is unique, and may permit companies to deflect lawsuits, including by curing violations of potential class representatives one-by-one.

That said, the CCPA does not provide guidance on what, exactly, would cure consumer injury following a data breach. The term "cure" is undefined in the statute, and the CCPA does not otherwise explain what remedy is appropriate after a consumer's data is accessed or taken without authorization. Given this ambiguity, a similar law with a cure period, the California Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750 *et seq*., may influence how the CCPA is interpreted.

The CLRA covers unfair and deceptive acts related to the sale of goods and services, and it prohibits damages under the statute when, among other things, a company "makes an appropriate correction, repair or replacement or other remedy of the goods and services" at issue. Cal. Civ. Code § 1784. Courts have interpreted offers to pay for damages resulting from the alleged CLRA violation as sufficient to satisfy its cure provision. This suggests that companies faced with a CCPA notice should consider offering the consumer payment of either reasonable statutory damages, or an amount tailored to the consumer's potential or actual damages, including attorneys' fees, as a cure for the alleged violation. Free data-monitoring services or indemnification agreements (related to damages in the event of future fraud on the consumers' account) provide other creative avenues to cure the violation.

In addition, companies may respond to a CCPA notice by fixing the specific security issue that caused the incident, and promising to do better in the future by instituting stronger security controls. While these may be important components to any cure, they are unlikely to be sufficient on their own. If future compliance alone were adequate, presumably every CCPA violation could be cured. The CCPA's safe harbor suggests otherwise. It expressly applies only "[i]n the event a cure is possible." As a result, going forward companies will need to critically assess whether to attempt to cure a violation with promises and new procedures aimed at future compliance alone.



III. Companies Should Take Steps Now to Reduce the Risk of Litigation Once the CCPA Takes Effect

Now is the time for companies to prepare to mitigate the substantial litigation risk that the CCPA presents. Encryption and redaction are a company's first line of defense against CCPA claims. Where only redacted or encrypted personal data is affected by a breach, a consumer cannot bring a CCPA claim (nor is a breach notification required). Thus, where technologically feasible, companies should encrypt consumers' personal data.

There are also other, less high-tech ways to minimize potential liability under the CCPA. A company's terms and conditions should include an arbitration provision and class action waiver, which may prevent CCPA class actions entirely. Although the CCPA purports to prohibit such waivers, *see* Cal. Civ. Code § 1798.192, the Federal Arbitration Act is likely to preempt that provision. To maximize enforceability, the terms and conditions should be conspicuously presented to consumers, and should require affirmative consent before a consumer provides any personal information. Moreover, the arbitration and class action waiver provisions within the agreement should be clear and concise, prominent and emphasized, and ideally, located in close proximity to the request for consent.

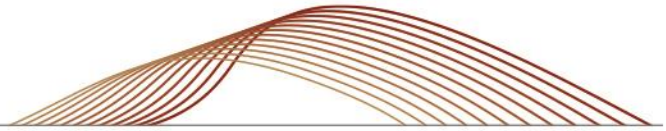
Next, companies should work with their internal and external counsel to assess their cybersecurity programs and those of relevant and important third parties or vendors to ensure that they have identified and remediated security deficiencies that may be deemed "unreasonable" under the law. Although the CCPA does not define "reasonable security procedures," industry norms and enforcement precedents are likely to establish the line between illegal and adequate protection in any litigation. A cybersecurity assessment can help a company determine how its procedures measure up.

Furthermore, companies should implement or modify their security breach response plans to anticipate notices to cure under the CCPA. This should involve creating a corporate intake and communications plan in response to notices to cure in the wake of a breach, along with an external plan, which may involve providing related contact information on a company's website or in future breach notifications. Responding timely to every notice to cure will be vital to reducing the possibility of classwide claims. Although the precise cure to a breach will be heavily fact-dependent and the law does not provide much guidance at this point, what is clear is that a failure to respond within 30 days will waive a key opportunity to effectively manage litigation risks that will go into effect in 2020.

Finally, cyber insurance may offer significant protection in the event a CCPA litigation proceeds. Existing and new policies should be carefully reviewed to ensure that CCPA actions are covered, and that the coverage limits are appropriate in light of the possible damages under the CCPA.

For a variety of reasons, it may be impractical for a company to take one or several of these steps, but proactively making even a few of these changes may substantially reduce a company's damages exposure under the CCPA.

✧ ✧ ✧



Paul Hastings LLP has a multi-disciplined group of lawyers and data scientists dedicated to working with clients to address CCPA and cybersecurity risks that are prevalent in numerous industries. If you would like more information, please contact one of the professionals below:

San Francisco

John P. Phillips
1.415.856.7027
johnphillips@paulhastings.com

Danielle D. Decker
1.415.856.7227
danielledecker@paulhastings.com

Washington, D. C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com