HUNTON ANDREWS KURTH

Lawyer Insights

The California Consumer Privacy Act is HERE: Are You Litigation Ready?

By Ann Marie Mortimer, Jason J. Kim and Lisa J. Sotto
Published in Cybersecurity Law & Strategy | April 1, 2020

Most companies doing business in California are well aware of the California Consumer Privacy Act of 2018 (CCPA) and prepared diligently in advance of the law's Jan. 1, 2020 compliance deadline. While compliance certainly is key, even compliant businesses must consider — and prepare for — the eventual onslaught of class action litigation that is coming.

Indeed, at least one data breach class action lawsuit has been filed already that expressly claims a "deprivation of rights" under the CCPA based on the alleged "fail[ure] to maintain reasonable security procedures and practices appropriate to the nature of" personal information maintained by the defendants. *Barnes v. Hanna Andersson, LLC, et al.*, N.D. Cal. Case No. 3:20-cv-00812. While the plaintiff in *Barnes* does not presently seek damages under the CCPA, she expressly "reserve[s] the right to amend this Complaint as of right" to do so at a later time. The plaintiff's decision not to seek damages under the CCPA likely stems from the retroactivity hurdles she would face, given the data breach "occurred from September 16, 2019 to November 11, 2019," and the relevant provisions of the CCPA are not expressly retroactive. *Weinberg v. Valeant Pharm. Int'l,* 2017 WL 6543822, at 7 (C.D. Cal. Aug. 10, 2017) ("California statutes apply prospectively unless the Legislature expressly indicates otherwise."). Nonetheless, the allegations highlight the looming threat on the horizon.

As background, the CCPA expands consumer data rights relating to the access to, deletion of, and "sale" of personal information collected by businesses. The CCPA also creates a private right of action that allows for the recovery of statutory damages ranging from $100 to $750 in the event of data breaches, which now are ubiquitous. Accordingly, if a breach affects just 100,000 California customers, the statutory damages quickly multiply, making claims under the CCPA attractive to the plaintiffs' bar.

How Does the New Law Change Things?

The plaintiff's bar has formed a cottage industry suing businesses that fall victim to data breaches — and they did so long before the passage of the CCPA. So what is new?

For one thing, the CCPA may make it more difficult to dispose of data breach lawsuits at the pleading stage, including the ability of the plaintiff to plead cognizable harm, as well as the difficulty in adjudicating the reasonableness of a business' security practices as a matter of law when limited to the facts alleged. Right out of the gate, businesses often would test the strength of a plaintiff's pleadings with respect to cognizable harm — a prerequisite to typical data breach claims and a threshold to federal court jurisdiction under Article III of the Constitution.

This article presents the views of the authors, which do not necessarily reflect those of Hunton Andrews Kurth LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article. Receipt of this article does not constitute an attorney-client relationship. Prior results do not guarantee a similar outcome. Attorney advertising.

But the CCPA potentially undercuts those arguments by allowing statutory damages. Businesses might argue that the United States Supreme Court's decision in ***Spokeo v. Robins***, 136 S.Ct. 1540 (2016), requires a plaintiff to plead and prove injury-in-fact beyond a bare statutory violation. Moreover, typical data breach claims require a *prima facie* showing of cognizable damages. However, numerous courts have provided plaintiffs with fodder to claim data breach victims face sufficiently imminent harm to constitute cognizable harm and to confer Article III standing, depending on the particular facts of the case and the information allegedly compromised.

The CCPA's impacts likewise might be felt at the class certification phase. Following the Supreme Court's decision in ***Comcast Corp. v. Behrend***, 133 S. Ct. 1426, (U.S. 2013), plaintiffs faced an uphill battle certifying data breach claims for class treatment, particularly given the difficulty of proving damages could be measured on a class-wide basis through a common methodology. Plaintiffs, however, might argue the CCPA eases their burden, claiming statutorily-prescribed damages under the CCPA could be established and quantified on a class-wide basis more readily than the typical individualized harms claimed in data breach cases.

Although the CCPA provides for a private right of action in data breach cases only, plaintiffs might seek to assert claims under other provisions of the CCPA. Indeed, in California, plaintiffs routinely bring claims for statutory violations under California's unfair competition laws (Cal. Bus. & Prof. Code §17200), even in instances where the underlying statute does not provide for a private right of action. Plaintiffs do so under the "unlawful" prong of Section 17200, which provides for restitution and injunctive relief when a defendant violates the law and the plaintiff suffers injury in fact. Section 1798.150 of the CCPA expressly states that nothing therein "shall be interpreted to serve as the basis for a private right of action under any other law." But that provision, of course, remains untested in litigation. Notably, California precedent has permitted Section 17200 claims to proceed under the "unlawful" prong even where the statute allegedly violated does not create a private right of action.

The CCPA does provide businesses an opportunity to cure. In particular, plaintiffs seeking statutory damages must notify a business of the alleged violation. If the business cures the violation within 30 days and states that no further violations will occur, the plaintiff will be barred from pursuing statutory damages. While sounding promising in theory, what constitutes an adequate cure in the context of a data breach remains uncertain and untested through litigation. How does a business "cure" a data breach that already occurred?

How Do Businesses Limit Exposure Under This Looming Threat?

While business will want to ensure they are CCPA-compliant, compliance alone will not prevent a plaintiff from filing suit under the CCPA. Indeed, no amount of preparation can ensure a company will not fall victim to a data breach.

But companies are not necessarily left defenseless. One tool to limit or otherwise avoid class action exposure is the use of an arbitration agreement that contains a class action waiver. Of course, an arbitration agreement will not be practical for every business — *e.g.*, a restaurant or brick-and-mortar retailer that collects payment card data when it accepts such cards for payment.

It should be noted that Section 1798.192 of the CCPA contains language that arguably purports to prohibit class action waivers as contrary to public policy. But the Federal Arbitration Act (FAA) likely preempts that provision under settled United States Supreme Court precedent, which repeatedly has rejected state law attempts to circumvent arbitration agreements.

Companies, therefore, should include arbitration agreements that contain class action waivers where practicable. To stave off challenges to the enforceability of such agreements, companies should ensure customer assent to such agreements is readily provable, and they should be mindful of the overall conscionability of the agreements. Among other provisions, the terms of such agreements should be presented in a clear and conspicuous manner with prominently displayed text. The terms should be mutual and reciprocal in nature so as not to appear one-sided. Customer assent should be requested and obtained in close proximity to the relevant provisions themselves, leaving no doubts that the terms were presented to the customer and accepted. With respect to online terms, for example, the customer ideally would be forced to scroll through terms containing the arbitration provision and affirmatively assent by clicking that he or she "accepts" them.

To the extent they have not done so already, companies also should take steps to implement "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Cal. Civ. Code §1798.150. Although the plaintiffs' bar challenged the reasonableness of businesses' security measures before the passage of the CCPA under other laws — *e.g.*, California's Customer Records Act and common law negligence — plaintiffs likely will cite the CCPA in addition to those theories now, as the *Barnes* complaint demonstrates. The CCPA does not define those "security procedures and practices" that meet the reasonableness standard. The plaintiffs' bar likely will rely on that omission to argue that the reasonableness of a company's security measures cannot be decided as a matter of law — and consequently, should be tried before a jury. But businesses have a counterargument. In **California's 2016 Data Breach Report**, then-Attorney General Kamala Harris stated that the "20 controls in the Center for Internet Security's Critical Security Controls [CIS 20] identify a minimum level of information security that all organizations that collect or maintain personal information should meet." Harris went on to state that the "failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." Absent further clarification from the California AG or otherwise, businesses might argue, based on Harris' statement, that the CIS 20 serves as a baseline for the CCPA's "reasonable security procedures and practices" element. Another potentially defensible benchmark might include the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST), the non-regulatory agency involved in the development of industry and scientific standards. Indeed, the Federal Trade Commission has **endorsed the NIST Cybersecurity Framework**, describing it as "consistent with the process-based approach that the FTC has followed since the late 1990s …." Similarly, Ohio law creates a safe harbor from data breach claims for businesses with cybersecurity programs that "reasonably conform[]" to certain recognized frameworks. Ohio Rev. Code Ann. §1354.03(A)(1)(a)-(f) (listing the **NIST Cybersecurity Framework**, **NIST Special Publication 800-171**, **NIST Special Publications 800-53** and **800-53a**, the **Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework**, the Center for Internet Security (CIS) **Critical Security Controls for Effective Cyber Defense**, the International Organization for Standardization/International Electrotechnical Commission **27000 Family — Information Security Management Systems**). Those too might serve as defensible frameworks under the CCPA.

As stated above, plaintiffs must give defendants 30 days' written notice and an opportunity to cure before they can recover statutory damages under the CCPA. Businesses that have implemented one or more of the foregoing benchmark measures should note the same in response to such a notice. For those businesses that have not, they should consider doing so (and communicate that in their response to a CCPA notice letter). Of course, businesses should consider whether their security procedures are otherwise defensible, even if they do not strictly follow the above-mentioned frameworks. A plaintiff might attempt to use a business' offer to "cure" as an admission that its security measures are not reasonable.

While the waters of CCPA litigation remain untested and uncharted, there are steps companies can take now to curb litigation exposure.

***Ann Marie Mortimer** co-heads the commercial litigation practice and is a managing partner and founder of the Los Angeles office. She is the lead litigation counsel on multiple large data breach cases, including what has been reported as the largest data breach in history. Her commercial litigation experience focuses on data security, false advertising and unfair competition class actions. She can be reached at +1 (213) 532-2103 or amortimer@HuntonAK.com.*

***Jason J. Kim** is counsel in the firm's commercial litigation group in the firm's Los Angeles office. His practice focuses on class action defense and other complex commercial litigation in the data breach, financial services and consumer contexts. He can be reached at +1 (213) 532-2114 or kimj@HuntonAK.com.*

***Lisa J. Sotto** chairs Hunton Andrews Kurth's Global Privacy and Cybersecurity practice, is the managing partner of the firm's New York office, and serves on the firm's Executive Committee. Lisa has advised clients on more than 1,700 cybersecurity and data breach incidents in the U.S. and abroad, including many of the seminal events, and was voted the world's leading privacy advisor in all surveys by* Computerworld *magazine. She can be reached at +1 (212) 309-1223 or lsotto@HuntonAK.com.*