Bloomberg Law

Professional Perspective

# CCPA Litigation Trends

*Lothar Determann and Teresa Michaud,*
*Baker McKenzie*

# CCPA Litigation Trends

*Contributed by Lothar Determann and Teresa Michaud, Baker McKenzie*

On July 1, 2020 California's attorney general started enforcing the California Consumer Privacy Act by sending letters to companies with requests to cure alleged violations, as contemplated by the CCPA. The legislation took effect on Jan. 1, 2020, as part of the California Civil Code, and called on the attorney general to enforce the law within six months of enacting regulations or July 1, 2020 the latest. The CCPA regulations became final only on Aug. 14, 2020, and the attorney general announced that they would apply with immediate effect on the same day.

Despite a seemingly clear division between the domains of government and private enforcement, plaintiffs' attorneys have been busy exploring ways that the CCPA can supply a basis for private civil litigation outside the data breach context. Whether private plaintiffs will be successful in this attempted expansion of the CCPA remains to be determined, but current trends in CCPA litigation can provide insight on what might be in store. This article explores those trends.

Within the CCPA, subsection (a) of Cal. Civ. Code § 1798.150 creates a narrowly framed right to private action in case of certain security breaches and clarifies in subsection (c) that aside from this one cause of action, "nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." By design, the CCPA vests enforcement authority in the attorney general.

We begin by examining a few selected lawsuits asserted under the data breach private right of action (Cal. Civ. Code § 1798.150), as the statute expressly contemplates. We then summarize some of the CCPA-related legal theories in non-data breach lawsuits, grouped generally into three main categories: unfair competition law claims based on underlying violations of the CCPA, negligence per se claims incorporating various apparent CCPA standards of care, and actions asserted directly under the CCPA.

Certainly, courts will have to determine whether these non-data breach legal claims can survive demurrer or motions to dismiss. None of the cases discussed herein have progressed yet to the extent that defendants have filed meaningful responsive pleadings, such as an answer to the allegations or a motion to dismiss pursuant to Rule 12(b)(6), much less to the point where a court decision has been issued.

## Data Breach Claims Under Private Right of Action

Cal. Civ. Code § 1798.150(a) of the CCPA allows any California resident to institute a civil action for monetary and injunctive relief if their personal information (a narrow category defined by the act) is subject to the "unauthorized access and exfiltration, theft, or disclosure as 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 to protect the personal information," circumstances commonly referred to as a "data breach." The following lawsuits have asserted data breach claims under section 1798.150.

***In re: Hanna Andersson, et al. Data Breach Litigation***, N.D. Cal. (Master File No. 3:20-cv-00812)

The plaintiffs in this consolidation action seek to represent a nationwide class, as well as a California sub-class of customers whose names, addresses and credit card information were allegedly exposed, "scraped," and offered for sale on the "dark web" following an alleged data breach suffered by Hanna Andersson in 2019, before the CCPA took effect. The plaintiffs' section 1798.150 claim alleges that the defendants failed to prevent the plaintiffs' and California sub-class members' unencrypted and non-redacted personally identifiable information (PII) from "unauthorized access and exfiltration, theft, or disclosure." The plaintiffs sued not only Hanna Andersson, with whom they had direct business dealings, but also a service provider, with whom the plaintiffs had no contractual or other relationships, despite the fact that the CCPA imposes obligations and liability only on businesses, not their service providers.

The plaintiffs alleged injuries including: "lost or diminished value of PII," "out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII," "lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to lost time," "deprivation of rights they possess under … the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, et seq.)," and "the continued and certainly an increased risk to their PII."

 

On Aug. 17, 2020, before the defendants had even filed a Rule 12 motion or otherwise responded to the plaintiffs' substantive allegations, the court stayed the case for 30 days following the parties' notice of settlement.

***Fuentes v. Sunshine Behavioral Health Group, LLC***, C.D. Cal. (Case No. 8:20-cv-00487)

The plaintiff here alleges that Sunshine, a drug and alcohol rehabilitation facility, allegedly violated the CCPA in connection with an alleged data breach that occurred in September 2019, before the CCPA took effect, and allegedly exposed the sensitive personal and medical information of approximately 3,500 patients. The named plaintiff is not a California resident, but a resident of Pennsylvania who was in California when the alleged breach occurred, and seeks relief under section 1798.150 in addition to California's Confidentiality of Medical Information Act (CMIA).

The plaintiff further seeks class-wide injunctive relief "in the form of an order enjoining Defendant from continuing to violate the CCPA." The complaint continues that should Sunshine not respond to the plaintiff's CCPA violation notice letter and rectify the alleged violation, the plaintiff "will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations." Notably, Cal. Civ. Code § 1798.145(c)(1) states that CCPA shall not apply to personal information governed by CMIA or HIPAA.

***Brodsky v. Ambry Genetics, Corp.***, C.D. Cal. (Case No. 8:20-cv-00811)

The plaintiff asserts a putative class action based on the alleged inadvertent disclosure of HIPAA-protected consumer information, including patients' names, dates of birth, health insurance information, medical information, and for some patients, Social Security numbers, and other sensitive personal information and Protected Health Information (PHI). While the complaint references that the plaintiff, "on behalf of all others similarly situated, alleges claims for … violation of the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, et seq. (§ 1798.150(a))),"  it stops short of actually seeking monetary or injunctive relief under the CCPA's private right of action.

Nevertheless, the court in June 2020 ordered that the *Brodsky* complaint be consolidated with three other related actions against the same defendant, which may well lead to an amended pleading that includes a standalone section 1798.150 claim. Again however, Cal. Civ. Code § 1798.145(c)(1) states that CCPA shall not apply to personal information governed by CMIA or HIPAA.

***Cercas, et al. v. Ambry Genetics Corp.***, C.D. Cal. (Case No. 8:20-cv-00791)

This consolidated action consists of separate individual complaints alleging that the defendant, a genetic testing facility, failed to implement and maintain reasonable data security measures. At least one complaint asserts a claim against the defendant for violating the CCPA by noting that the unauthorized access of unencrypted and non-redacted personal and medical information was a result of the defendant's duty to implement and maintain such measures. The parties have proposed a deadline of Nov. 20, 2020 for the defendant to file a responsive pleading.

***Karter v. Epiq Systems, Inc.***, Orange County Superior Court (Case No. 30-2020-01145269)

The putative class action complaint in this case asserts a sole claim against a legal services technology provider for a violation of the CCPA. The plaintiff seeks relief under section 1798.150 for the defendant's alleged use of outdated data security measures, leading to various malware and ransomware attacks and the exfiltration of consumers' unencrypted and non-redacted personal information.

***Gupta, et al. v. Aeries Software, Inc.***, C.D. Cal. (Case No 8:20-cv-00995)

The plaintiffs, an individual and his minor children, assert claims against a software company that manages student-data for failing to implement adequate data security measures, failing to detect a data breach, and failing to maintain security systems consistent with industry standards. The complaint further alleges that the defendant owed a heightened duty to the plaintiffs as minors, and that the data security shortcomings resulted in a data breach of the minors' personal information. The plaintiffs rely on alleged violations of the CCPA to an unfair competition law claim in addition to their section 1798.150 data breach cause of action.

***California Unfair Competition Law Claims Asserting Violations***

California's unfair competition law provides a private right of action arising from, among other things, any "unlawful conduct." The plaintiffs have brought unfair competition law claims on the theory that defendants have acted unlawfully by

violating various aspects of the CCPA other than section 1798.150's data breach provisions. As indicated above, enforcement of these additional aspects of the CCPA is reserved for the California attorney general, not private litigants.

Indeed, section 1798.150(c) explains that the CCPA's private cause of action "shall not be based on violations of any other section" of the law, "nor shall a CCPA violation "be interpreted to serve as the basis for a private right of action under any other law." The statute therefore would seem clearly to bar a "private right of action under" the unfair competition law whose basis is an alleged violation of the CCPA. Yet this has not prevented plaintiffs from testing the boundaries of this straightforward statutory limitation.

***Burke, et al. v. Clearview AI, Inc., et al.***, S.D.N.Y., originally filed in S.D. Cal., case no. 3:20-cv-00370 (Case No. 1:20-cv-03104)

The plaintiffs allege that Clearview and its two founders used facial recognition technology to scrape social media websites for images of consumers' faces without their notice or consent, which they claim constitutes improper collection and sale of information protected by the CCPA. The plaintiffs' unfair competition law claim on behalf of various subclasses arises from the defendant's allegedly "unlawful" violation of the CCPA in collecting the class members' personal information without prior notice or consent. While the parties have battled over the proper venue for the case, the legal sufficiency of plaintiffs' unfair competition law claim has not yet been challenged.

***Hernandez v. PIH Health Inc.***, Los Angeles County Superior Court (Case No. 20STCV09237)

The plaintiff asserts a number of claims arising out of a targeted phishing campaign against PIH, a regional healthcare network. The complaint alleges that the cyberattack against PIH affected the plaintiff and approximately 200,000 other individuals, and resulted the unauthorized disclosure of the plaintiff's medical information. But instead of asserting a section 1798.150 data breach claim, the Complaint alleges that PIH's potential violation of the CCPA gives rise to liability under California's unfair competition law.

***Alizadeh, et al. v. Enloe Medical Center***, Butte County Superior Court (Case No. 20cv00799)

The plaintiffs in this case assert a host of claims against an operator of medical facilities in response to a ransomware attack against the defendant. The allegations state that the ransomware attack blocked access to highly sensitive patient medical records, and that putative class members suffered losses in the form of disrupted medical services and other expenses. The complaint alleges that failures to protect against the attack resulted in violations of multiple laws, including the CCPA, and that these violations in turn support an unfair competition law claim.

***Bombora, Inc. v. ZoomInfo Technologies LLC***, Santa Clara County Superior Court (Case No. 20CV365858)

In this case between two data brokers, the plaintiff alleges that the defendant, a former business partner, gains competitive advantages by violating the CCPA. Both companies sell so-called "intent" data, which purportedly attempts to predict consumers' future product purchases. The complaint alleges that the defendant does not include an opt-out notification regarding the data it collects within a "free" user application, and that this policy violates the CCPA and therefore supports a claim under unfair competition law. The defendant has filed a motion to dismiss arguing that a forum selection agreement between the parties mandates suit in federal or state court in New York, New York.

**Negligence Per Se Claims Alleging Violations of Statutory Duties of Care**

As described above, section 1798.150 of the CCPA allows private litigants whose data has been subjected to unauthorized access to seek damages arising from a business's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." This is, in effect, a statutory duty of care—albeit bereft of any clear guidance as to what constitutes "reasonable security procedures and practices"—which could theoretically provide the basis for a common law "negligence per se" theory of liability.

Indeed, in the *Hanna Andersson* litigation discussed above, one of the plaintiffs originally included a claim sounding in negligence per se, alleging that the defendants had breached section 1798.150's duty of care in the protection of consumers' personal information. The plaintiff subsequently voluntarily dismissed that claim, presumably because the CCPA provides for statutory damages; in common law negligence claims involving data breach events, proving causation and damages can be very difficult.

The cases described below have asserted a similar theory of negligence liability. We believe, however, that such claims should be subject to dismissal for the same reasons discussed above in connection with unfair competition law: the CCPA by its own terms may not "be interpreted to serve as the basis for a private right of action under any other law," including the common law of negligence.

***Henrichsen, et al. v. Tandem Diabetes Care, Inc.***, S.D. Cal. (Case No. 3:20-cv-00732)

This putative class action is brought by an Illinois plaintiff, her minor son, and a California plaintiff against a medical device manufacturer. The plaintiffs allege that a phishing attack caused a data breach, and they accuse the defendant manufacturer of failing to implement and maintain reasonable security procedures and practices to prevent such a breach. The plaintiffs assert a section 1798.150 data breach cause of action, as well as claims for negligence and unfair competition law violations predicated on alleged CCPA violations. On May 22, 2020, the plaintiffs voluntarily dismissed their lawsuit, but without prejudice to refile it in the future.

***Atkinson, et al. v. Minted, Inc.***, N.D. Cal. (Case No. 3:20-cv-03869)

The plaintiffs here seek to represent a consumer class against the defendant, an online marketplace for "crowd sourced" home goods, for an alleged data breach and disclosure of their PII. In addition to asserting a section 1798.150 data breach claim, the plaintiffs rely upon the duties imposed under the CCPA to accuse the defendant of negligence per se. The plaintiffs also assert an unfair competition law claim based on alleged CCPA violations.

***Juan Flores-Mendez, et al. v. Zoosk Inc., et al.***, N.D. Cal. (Case No. 3:20-cv-04929)

Two plaintiffs allege that the defendant, the creator and manager of an online dating app, failed to implement and maintain reasonable security measures, which resulted in the hacking and theft of users' information. The complaint alleges that putative class members must constantly monitor personal records as a result of the data breach and that they are now at higher risk of phishing and pharming attacks. The plaintiffs include a claim under the CCPA itself for the company's alleged failures, but additionally use the statute to support negligence and unfair competition law claims.

## Non-Data Breach Claims

In this last category of cases, the plaintiffs seek to base claims directly on allegations of defendant's failure to comply with the CCPA's consumer notification and consent provisions. The plaintiffs do not invoke unfair competition law or other causes of action to support their claims with indirect references to CCPA violations, as in the previously discussed group of cases, but plaintiffs refer directly to CCPA sections, despite the fact that Cal. Civ. Code § 1798.150(c) expressly and specifically precludes such claim.

***In re Ring LLC Privacy Litigation***, C.D. Cal. (Case No. 2:19-cv-10899)

This consolidated action includes class claims by a Washington consumer against a video doorbell and security camera manufacturer. At least one of the related cases (Case No. 20-cv-01538) includes a standalone cause of action for "violation" of the law for allegedly collecting and using personal information without providing consumer notice and an opportunity to opt out.

***Sweeney v. Life on Air,*** Inc., et al., S.D. Cal. (Case No. 3:20-cv-00742)

The California plaintiff here asserts claims on behalf of a putative class against two companies behind a social networking application that allows for multiple users to video chat simultaneously. The complaint alleges that the companies violated the CCPA by disclosing users' PII to unauthorized third parties, including advertisers, without providing the required notice to and consumers and giving them a right to opt out. Interestingly, despite its many CCPA-related allegations, the complaint does not rely on that statute in asserting liability under California's unfair competition law. The defendants have responded by filing a motion to compel arbitration or alternatively transfer the case.

***L.P., et al. v. Shutterfly Inc.***, N.D. Cal. (Case No. 3:20-cv-04960)

A group of minors brought suit against the defendant, an online image sharing platform, for alleged violations regarding the company's facial recognition software. The plaintiffs allege that the company used the software on users and non-users to "tag" them in photos without consent, concealed its use of the software, failed to disclose the collection of biometric data, and then sold personal information of minors to third parties. The complaint asserts a direct violation of CCPA on the

theory that the "sale of personal information of minors *equates to that of a data breach*," thereby stretching the statutory definition of data breach past its likely breaking point.

## Insights from Pending Cases

In the cases filed to date, the plaintiffs' attorneys have not advanced any compelling arguments why the clear limitations on private actions in the CCPA should not apply and preclude the claims. The claims based on unfair competition law and negligence per se clearly fall within the CCPA prohibition that "Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Courts have not yet allowed any such cases to proceed in litigation past the motion to dismiss stage.

*Ed Totino, Alex Davis, Sara Pitt, Gary Hunt, and Tom Tysowsky contributed to this article.*