Key Developments in CCPA Litigation for Q1 2021

Alysa Z. Hutnik

May 4, 2021

As we move deeper into the second year of CCPA litigation, the substantive issues continue to develop and we remain focused on the patterns and implications of recent filings and rulings. In this post, we highlight notable developments in three cases that occurred in the first quarter of 2021. These cases raise significant issues regarding judicial interpretation of the private right of action in the CCPA, the definition of a "data breach," and CCPA plaintiffs' ability to access pre-complaint discovery.

CCPA Claim Dismissed For Lack Of Data Breach Allegations

On August 5, 2020, Plaintiff filed a class action complaint against Defendants Alphabet, Inc. and Google, LLC in the Northern District of California. Plaintiff alleged that Defendants monitored and collected Android Smartphone users' sensitive personal data without those users' consent when they interacted with non-Google applications on their smartphones. Plaintiff's CCPA cause of action was based on Defendants' failure to disclose these activities in violation of Cal. Civ. Code § 1789.100(b). Plaintiff's proposed class definition included "All Android Smartphone users from at least as early as January 1, 2014 through the present."

On September 30, 2020, Defendants moved to dismiss the CCPA claim, arguing that (1) Plaintiff failed to allege that his information was subject to a data breach; and (2) Plaintiff, as a New York resident, had no standing under the CCPA, which only provides relief to California residents.

On February 2, 2021, the court dismissed the CCPA claim with prejudice, finding that the complaint did not allege that any personal information was subject to unauthorized access as a result of a security breach. The court reasoned that the CCPA only conferred "a private right of action" for violations related to "personal information security breaches," and that Plaintiff was therefore unable to state a claim. The court also observed that Civil Code § 1798.150(c) explicitly states that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law." *McCoy v. Alphabet, Inc.*, No. 20-CV-05427-SVK, 2021 WL 405816 (N.D. Cal. Feb. 2, 2021).

On February 16, 2021, Plaintiff filed an Amended Complaint that alleges a violation of California's Unfair Competition Law ("UCL") using the alleged CCPA violation as a predicate. It will be relevant to follow how the court addresses Plaintiff's attempt to transform his dismissed CCPA claim into a UCL

claim, in light of the court's observation that the CCPA does not provide a basis for a private right of action under other laws.

McCoy v. Alphabet, Inc. et al., 5:20-cv-05427 (N.D. Cal.).

Plaintiffs Allege Numerous, Individualized "Data Breaches"

On April 1, 2021, Plaintiffs filed a Consolidated Class Action Complaint against Bank of America in the Northern District of California. Plaintiffs allege that Bank of America issued Visa debit cards containing public benefit disbursements to recipients, including Plaintiffs and other members of the class, that were purportedly prone to breaches because the cards utilized outdated magnetic stripe technology, rather than the EMV chips that have allegedly become the industry standard due to improved security features. Plaintiffs' CCPA cause of action alleges that as a result of the inadequate security safeguards, the cardholders suffered unauthorized access and disclosure of their personal information that resulted in their funds being stolen through unauthorized transactions.

The statutory language of the CCPA indicates that a claim must be connected to a data breach. Cal. Civ. Code § 1789.150. Unlike most cases, Plaintiffs do not allege that a single, centralized data breach occurred. Instead, Plaintiffs allege that individual data breaches of each cardholder were permitted by Bank of America's card design. This theory raises questions about what qualifies as a data breach under the CCPA and whether the design of a consumer product that renders the product vulnerable to breach, followed by actual breaches, qualifies. A judicial determination of this issue could help determine the scope of similar consumer actions.

Yick v. Bank of America, N.A., 3:21-cv-376 (N.D. Cal.).

Defendant Compelled To Disclose Information Related To Data Breach Investigations

On April 16, 2021, Plaintiffs filed a redacted Consolidated Class Action Complaint against Blackbaud, Inc. in the District of South Carolina. Plaintiffs allege that Blackbaud provides data security services for sensitive information, and that Plaintiffs and the class members are Blackbaud's clients. Plaintiffs' CCPA cause of action alleges that as a result of a data breach, cybercriminals stole the sensitive private information that Plaintiffs entrusted to Blackbaud.

Of note, the early proceedings in this case have included the forced production of Blackbaud's forensic report on the data breach. The report was apparently compiled independent of the litigation and, upon learning of the report, the Court ordered Blackbaud to immediately produce the forensic report and allowed Plaintiffs to use that report in drafting a consolidated complaint. This is an issue that we've explored previously (here and here). Companies need to be vigilant and deliberate in how they approach the issue of internal investigations concerning data breaches where litigation could arise.

In re Blackbaud, Inc., Customer Data Breach Litigation¸ 3:20-mn-02972-JMC, MDL No. 2972 (D.S.C.).

As these and other CCPA-related cases progress through the litigation stages, we will continue to provide updates. Our prior summaries of CCPA-related litigation can be found in our CCPA Litigation Round-ups for: Q1 2020, Q2 2020, and Q3 & Q4 posts. We will continue to report on relevant developments in CCPA litigation and provide updates in our CCPA Litigation Tracker.

If you have any questions about defending and/or preparing for a potential privacy consumer class action, please reach out to our team, and if you have questions on your privacy compliance strategy, please reach out to our privacy compliance team.

On the latest episode of the Ad Law Access Podcast, Kelley Drye Partner Alysa Hutnik discusses the state of privacy, tracking, compliance technology and tools, and strategies privacy lawyers and others can use to help do their jobs. As you would expect, there are some practical tips to take away. Listen here or wherever you get your podcasts.