CCPA Litigation Round-Up: Q3 & Q4 2020

Alysa Z. Hutnik

January 22, 2021

It has been a full year since the California Consumer Privacy Act ("CCPA") took effect at the top of 2020. In the cases filed in the second half of the year, the complaints more frequently assert a violation of the CCPA as a standalone cause of action, though it remains common for a CCPA violation to be asserted as a predicate to support a separate cause of action, such as a violation of California's Unfair Competition Law ("UCL").

In this post, we include our round-up of representative cases filed in the third and fourth quarters of the year. Our prior summaries of CCPA-related litigation filed last year can be found in our Q1 2020 CCPA Litigation Round-Up and CCPA Litigation Round-Up: Q2 2020. We have separately analyzed trends emerging from the 2020 CCPA litigation landscape. Going forward into 2021, we will continue to report on relevant developments in CCPA consumer litigation, and also provide updates in our CCPA Litigation Tracker chart.

1. **Cases Filed in Q3/Q4 2020 Alleging Direct Violation of CCPA**

Shadi Hayden v. The Retail Equation, Inc. et al., No. 8:20-cv-01203 (C.D. Cal.)

On August 3, a class action amended complaint was filed by thirteen named plaintiffs against The Retail Equation, Inc. ("TRE") and a variety of retailers: Sephora USA, Inc., Advance Auto Body Parts, Inc., Bed Bath & Beyond, Inc., Best Buy Co., Inc., Buy Buy Baby, Inc., Caleres, Inc., CVS Health Corporation, Dick's Sporting Goods, Inc., L Brands, Inc., Stein Mart, Inc., The Gap, Inc., The Home Depot, Inc., and The TJX Companies, Inc. (the "Defendant Retailers") in the District Court for the Central District of California. Plaintiffs' CCPA claim alleges that the Defendant Retailers, without their customers' knowledge or consent, collect large amounts of data about their retail customers, including: (1) "Consumer Commercial Activity Data," which includes "the unique purchase, return, and/or exchange histories of individuals consumers"; and (2) "Consumer ID Data," which includes "the unique identification information contained on or within a consumer's driver's license, government-issued ID card, and/or passport" such as "the consumer's name, date of birth, race, sex, photograph, complete street address, and zip code." Plaintiffs allege that this data is shared with TRE as non-anonymized, individual data sets, which TRE processes to create consumer reports and a risk score for each customer. The risk score is allegedly used to advise the retailer about whether a customer's attempted return or exchange is fraudulent or abusive. The amended complaint alleges that "Defendants' policies and practices failed to hold plaintiffs' and Class members' personal information secure by, for example, [the Retailer Defendants' sharing of] the personal information . . . in an unsecured, unrestricted manner with TRE to create consumer reports and generate a 'risk score' that TRE then shared with other Defendant Retailers alongside other personal information."

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

On August 5, 2020, plaintiff Robert McCoy filed a class action complaint against defendants Alphabet Inc. and Google LLC for monitoring and collecting the sensitive personal data of Android Smartphone users when they interact with non-Google applications on their smartphones, without obtaining consent. This personal data includes the duration of time spent on non-Google apps and how frequently those apps are opened. Plaintiff's CCPA cause of action alleges that defendants failed to disclose that they collect the class members' personal data and the true purpose for collecting the data, which plaintiff alleges is to gain a competitive edge over rival companies. Plaintiff's proposed class definition includes "All Android Smartphone users from at least as early as January 1, 2014 through the present."

On September 30, 2020, Google filed a Motion to Dismiss, including arguments that the CCPA claim fails because (1) plaintiff fails to allege his information was subject to a data breach; and (2) relief is only available to a consumer, which is defined as a "California resident," and plaintiff is a New York resident.

Guzman v. RLI Corp. et al., No. 2:20-cv-08318 (C.D. Cal.)

On September 10, 2020, plaintiff Jose Guzman filed a class action complaint against defendants RLI Corp. and RLI Insurance Company alleging that defendants, through the Pacer filing service, disclosed the login credentials to computer systems containing personal and confidential information of class members. Plaintiff alleges that as a surety, defendants requested access to the records of Libre by Nexus, which secures bonds for detained undocumented immigrants. Plaintiff alleges that, in a separate suit, defendants disclosed Libre's login credentials by filing them publicly, giving anyone with a Pacer login access to class members' personal and confidential information including dates of birth, names of minor children, home address, Social Security Numbers, and taxpayer identification numbers and financial account information.

On October 22, 2020, defendants filed a Motion to Dismiss, including arguments that the CCPA claim fails because: (1) defendants' access was court-authorized and therefore not unauthorized; (2) plaintiff failed to establish that there was a "violation of the duty to implement and maintain reasonable security procedures and practices"; and (3) plaintiff did not comply with the mandatory 30-day notice and cure provision. On November 6, 2020, the action was voluntarily dismissed without prejudice.

Gardiner v. Walmart Inc. et al., 4:20-cv-04618 (N.D. Cal.)

On July 10, 2020, plaintiff Lavarious Gardiner filed a class action complaint against retailer Walmart alleging that vulnerabilities on Walmart's website led to breaches of Walmart's systems, allowing hackers to steal customers' personally identifiable information (including full names, addresses, financial account information, and credit card information), and allowed hackers to attack Walmart's customers' computers directly as well. The CCPA cause of action alleges that Walmart violated its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information. On October 29, 2020, the Parties stipulated to a briefing schedule on defendant's Motion to Dismiss which is scheduled to be completed by February 3, 2021.

Flores-Mendez et al v. Zoosk, Inc. et al., 3:20-cv-04929 (N.D. Cal.)

On July 22, 2020, plaintiffs Juan Flores-Mendez and Amber Collins filed a class action complaint against Zoosk, Inc., an online dating site, and its parent company, Spark Networks SE, alleging that cybercriminals hacked and obtained 30 million of Zoosk's user's records, containing their name, email, date of birth, and password, due to Zoosk failing to maintain reasonable security controls and

systems. Plaintiffs only sought injunctive and equitable relief but alleged that if Zoosk could not cure the breach within 30 days of its July 14 notice letter, they intended to amend to seek actual and statutory damages. On October 30, 2020, plaintiffs filed an Amended Complaint.

Warshawsky et al v. cbdMD, Inc et al., No. 3:20-cv-00562 (W.D.N.C.)

On October 9, 2020, plaintiffs Michael Warshawsky and Michael Steinhauser filed a class action complaint against cbdMD Inc., and CBD Industries, LLC. Plaintiffs allege that due to two data breaches, hackers accessed consumers' names, credit card numbers, CVV security codes, credit card expiration dates, addresses, email addresses, and bank account numbers. Plaintiffs' CCPA cause of action alleges that defendants' computer systems and data security practices were inadequate to safeguard its customers' personal information.

Diczhazy et al v. Dickeys Barbecue Restaurants Inc. et al., No. 3:20-cv-2189 (C.D. Cal.)

On November 9, 2020, plaintiffs Ross Diczhazy and Wesley Etheridge II filed a class action complaint against Dickey's Barbecue Restaurants Inc. and Dickey's Capital Group, Inc. for their alleged failure to secure and safeguard the names, payment card numbers and security codes of proposed class members in a data breach in violation of the CCPA. The complaint purports two classes: (a) All California residents who made a purchase from Dickey's using a payment card, or otherwise disclosed payment card information to Dickey's, since January 1, 2020, and whose personal information was compromised including as part of the Joker's Stash BlazingSun data set; and (b) All persons who made a purchase from Dickey's using a payment card, or otherwise disclosed payment card information to Dickey's, since January 1, 2018, and whose personal information was compromised including as part of the Joker's Stash BlazingSun data set.

Marquez v. Dickey's Barbecue Resturants, Inc. et al., No. 3:20-cv-2251 (S.D. Cal.)

On November 18, 2020, plaintiff Jose Luis Marquez also filed a class action complaint against Dickey's Barbecue Restaurants Inc. and Dickey's Capital Group, Inc. for their failure to secure and safeguard their customers' personal identifying information. As in *Diczhazy* (above), there is a nationwide class as well as a California subclass alleged: (a) All persons residing in the United States who made a credit or debit card purchase at any affected Dickey's Barbecue Pit restaurant during the period of the Data Breach; and (b) All persons residing in the State of California who made a credit or debit card purchase at any affected Dickey's Barbecue Pit restaurant during the period of the Data Breach.

Gitner v. U.S. Bank National Association et al., No. 0:20-cv-02101 (D. Minn.)

On November 20, 2020, plaintiff Barry Gitner filed a first amended class action complaint in the District of Minnesota against U.S. Bank National Association and U.S. Bancorp for their alleged failure to secure and safeguard the confidential, personally identifiable information of thousands of consumers, including names, account numbers, Social Security Numbers, driver's license numbers, and dates of birth. Specifically, plaintiffs allege that a computer server with consumer information was stolen from defendants' corporate offices. Under the CCPA cause of action, plaintiffs seek injunctive or other equitable relief but reserve their rights to amend the complaint to seek actual and statutory damages if the breach is not cured within 30 days. On January 13, 2021, the Court stayed the action pending arbitration of Plaintiff's individual claims, after defendants' Motion to Compel Arbitration was unopposed.

Schaubach v. Hotels.Com, LP et al., No. 8:20-cv-2370 (C.D. Cal.)

On December 17, 2020, plaintiff Lauren Schaubach filed a class action complaint against defendants Hotels.com, L.P. ("HLP"), Expedia Group, Inc. ("Expedia") and Amazon Web Services, Inc. ("AWS") after a Cloud Hospitality server hosted by Defendant AWS and containing information for customers of Defendant HLP and Defendant Expedia was hacked and tens of millions of data records were exposed, including full names, email address, ID numbers, phone numbers, credit card numbers, security codes and expiration dates. Plaintiff seeks to represent a class of "all consumers in California whose personally identifiable information was compromised in the Breach." On December 17, 2020, the action was voluntarily dismissed without prejudice.

1. **Cases Filed in Q3/Q4 2020 Alleging CCPA Violations As a Predicate For UCL Causes of Action**

Pygin v. Bombas, LLC et al., No. 4:20-cv-04412 (N.D. Cal.)

On July 1, 2020, plaintiff Alex Pygin filed a class action complaint against defendants Bombas, LLC, Shopify (USA) Inc. and Shopify, Inc., alleging that sock and apparel retailer Bombas uses an ecommerce platform supplied by Shopify to take customers' personal and payment information (including name, billing, shipping and email addresses, along with credit card numbers, expiration dates, and security codes) and that the customers' information was compromised during a data breach due to defendants' negligent and/or careless acts and omissions and failure to protect the data.

While plaintiff brings no claim under the CCPA, he alleges that class members have suffered injury including "deprivation of rights they possess under . . . the California Consumer Privacy Act" by "failing to maintain reasonable security procedures and practices appropriate to the nature of the personally identifiable information." As part of its causes of action for negligence and violation of the UCL, plaintiff alleges that defendants: (i) had a duty to take reasonable steps and employ reasonable methods of safeguarding the personally identifiable information of class members, as required under the CCPA; (ii) failed to maintain those reasonable security procedures and practices by storing the information in an unsecure electronic environment; and (iii) failed to disclose the data breach to class members in a timely and accurate manner as required by the CCPA.

Currently pending before the Court is Shopify's Motion to Dismiss for (1) lack of personal jurisdiction, (2) violation of FRCP 8 for failing to distinguish among defendants and adequately allege that Shopify caused harm, and (3) failure to state a claim, based partially on the argument that the CCPA does not "create any private right of action under any other law."

Calixte et al. v. Dave, Inc., 2:20-cv-07704 (C.D. Cal.)

On August 24, 2020, five plaintiffs filed a class action complaint against defendant Dave Inc. alleging that its users' names, emails, date of birth, physical address, phone numbers and social security numbers were compromised as a result of a cyberattack against a former third party service provider of Dave Inc. The complaint alleges that the hackers' ability to pivot from a third-party vendor's system to the defendant's systems without detection demonstrates the lack of controls and cybersecurity measures in use at Dave Inc. to prevent such unauthorized use.

Plaintiffs only allege violations of the CCPA as a predicate to their UCL violation cause of action based on Dave Inc.'s alleged failure to implement and maintain reasonable security measures. The proposed nationwide class is defined as "All persons whose PII was compromised as a result of the Data Breach announced by Dave Inc. in July and August of 2020." The Parties are currently briefing defendant's Motion to Compel Arbitration. On November 9, 2020, the action was voluntarily

dismissed without prejudice.

Wesch v. Yodlee, Inc. et al., No. 3:20-cv-05991 (N.D. Cal)

On August 25, 2020, plaintiff Deborah Wesch filed a class action complaint against defendants Yodlee, Inc. and Envestnet, Inc. (who acquired Yodlee) alleging that Yodlee sells highly sensitive financial data, such as bank balances and credit card transaction histories, collected from software products that it markets and sells to financial institutions. Plaintiffs allege that when individuals connect their bank accounts to Paypal, they upload their banking credentials using Yodlee's system. Yodlee then allegedly stores a copy of the credentials on its own system and exploits them, contrary to the disclosed use of the information.

Plaintiff's UCL cause of action is predicated upon alleged violations of the CCPA, including that defendants: (i) disclose before or at the point of collection, the category of information to be collected and how it will be used; and (ii) refrain from collecting additional information for additional purposes without providing notice.

Plaintiff filed an Amended Complaint on October 21, 2020 and the parties have stipulated to briefing schedule on plaintiff's anticipated Motion to Dismiss.

Conditi v. Instagram, LLC et al., No. 3:20-cv-06534 (N.D. Cal.)

On September 17, 2020, plaintiff Brittany Conditi brought a class action complaint against defendants Instagram LLC and Facebook Inc. alleging that Instagram constantly accesses users' smartphone camera feature and monitors users without permission when they are not interacting with the camera feature, which goes beyond the services it promises to provide. Plaintiff alleges that Instagram does this to collect valuable personal data to increase their advertising revenue.

Plaintiff's UCL cause of action is based upon allegations that defendants violated the CCPA by failing to disclose that they monitor users through their smartphone cameras, while not in use, to collect personal information. Plaintiff proposes the following class definition: "All Instagram users whose smartphone cameras were accessed by Instagram without their consent from 2010 through the present (the 'Class Period')."

You can follow developments in CCPA-related cases by referring to our new 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.