STRADLEY RONON

Cyber & Privacy Alert | August 31, 2022

Sephora USA, Inc. Agrees to Pay $1.2 Million in Settlement With California Attorney General for Alleged Violations of CCPA

"I hope today's settlement sends a strong message to businesses that are still failing to comply with California's consumer privacy law. My office is watching, and we will hold you accountable."

– California Attorney General Rob Bonta

On Aug. 24, 2022, Attorney General Rob Bonta announced a $1.2 million settlement with beauty and cosmetics brand Sephora USA, Inc. The settlement aims to resolve claims that Sephora's e-commerce business failed to comply with California data privacy law. The settlement marks California's first public California Consumer Privacy Act (CCPA) enforcement action, coming over two years after the law first went into effect. The terms of the settlement have been submitted for court approval.

The proposed settlement was announced one day after the AG's office filed a complaint in the California Superior Court in San Francisco alleging that, among other things, Sephora failed to disclose to consumers that their data was being sold. The complaint further alleges that Sephora failed to provide a "Do Not Sell My Personal Informational" link or inform consumers of their right to opt-out of the sale of their data. The AG also alleges that Sephora's website was not configured to detect or process any global privacy control signals, a digital signal that allows users to communicate sales opt-out across platforms.

According to the AG's complaint, Bonta began an "enforcement sweep of large retailers" back in June of 2021, with a focus on ensuring that these retailers were responding to users' global privacy control signals. This investigation revealed Sephora's broader alleged non-compliance with CCPA. The AG sent Sephora notice of its potential CCPA violations last summer; however, the complaint further alleges that Sephora failed to take any corrective actions within the 30-day cure period currently provided under California law.

Like many other online retailers, Sephora's website and mobile app deployed third-party tracking software, providing Sephora with customer insights, and assisting in effective online advertising. The complaint alleges, however, that Sephora allowed these third-party companies access to its customers' browsing data to create profiles that would be used for their own purposes in exchange for discounted or higher-quality analytics or advertising, noting that "if companies make consumer personal information available to third parties and receive a benefit from the arrangement—such as in the form of ads targeting specific consumers—they are deemed to be 'selling' personal information under the law." The complaint alleged that "both the trade of personal information for analytics and the trade of personal information for an advertising option constituted sales under the CCPA." It further noted that Sephora had not taken action to put service-provider contracts in place with the providers of the analytic services, which would have acted as an exception to a sale under the CCPA. Per Sephora USA, Inc.'s privacy policy—dated

continued on next page

June 18, 2021—the customer information it collected and shared with third-party providers included its users' precise location data, and Sephora told its customers that "we do not sell personal information." In short, when Sephora provided access to its users' browsing data in exchange for discounted analytics, it triggered a number of CCPA compliance obligations that the AG alleges Sephora ignored.

The complaint further alleges that Sephora also failed to detect or process any of its customers' global privacy control signals as required by CCPA. User-enabled global privacy controls are browser extensions that allow customers to communicate sales opt-outs globally, saving the user from having to individually communicate their opt-out to each website or mobile application. Per the complaint, CCPA's requirement that businesses take steps to treat global privacy controls as an affirmative opt-out request was meant to "spur innovation and encourage the development of technologies that would allow consumers to universally opt-out of all online sales in one fell swoop." By allegedly disregarding users' "do not sell" signals while also failing to provide alternative methods to opt-out of the sale of their data, Sephora was alleged to have ignored CCPA's primary regulatory function; namely, allowing consumers to communicate to businesses to not sell their data to third parties.

The settlement with Sephora was announced amid increased efforts by AG Bonta to enforce CCPA. The Sephora enforcement action makes clear California's willingness to institute litigation against non-compliant companies and that there may be a hefty price tag for e-commerce activity that fails to comport with the requirements of CCPA.[1] Though the AG's decision to bring this action against Sephora USA, Inc.—a company amendable to suit in California under typical venue and jurisdictional principles—sidesteps the lingering question of California's ability to enforce CCPA against a company that operates entirely outside of that state, companies with potential exposure under CCPA should carefully consider the clear message that California has sent to CCPA-covered businesses across the country.

One strategy to avoid some of these issues is to execute CCPA-compliant service provider agreements with any third party that receives "personal information" relating to your customers. CCPA defines a "service provider" as a for-profit entity that processes personal information on your organization's behalf and who is, by contract, prohibited from retaining, using or disclosing that personal information for any purpose other than performing the services specified in the contract. Limiting a third party's use of your customer's personal information should provide a robust defense to a claim that the information sharing was a disguised "sale" under CCPA.

Companies should also ensure that their online platforms are set up to recognize and properly respond to users' global privacy signals. The complaint states that the investigation into Sephora was spurred on by the AG's larger inquiry into compliance with Global Privacy Control signals. In a statement regarding the settlement, Bonta said that "technologies like the Global Privacy Control are a game changer for consumers looking to exercise their data privacy rights." It is clear from the complaint that California intends to treat a company's non-response to a user's "do not sell" signal as no different than failing to honor a sale opt-out delivered through the other means provided under CCPA. It appears that encouraging broad adoption of Global Privacy Control signals is a priority for AG Bonta, and future enforcement actions are likely to reflect that priority.

Finally, companies should carefully review any agreement involving the sharing of personal data that does not include the use-limitation language described above. Sharing customers' personal information with a third party outside of a CCPA-compliant service provider agreement does not necessarily equal a "sale" of data. However, absent a compliant service agreement, the risk of an undisclosed quid pro quo exchange increases an organization's risk of regulatory enforcement for an undisclosed "sale" of personal information. Prior to this enforcement action, Sephora publicly informed its users that it did not sell their data. However, the CCPA's broad definition of "sale" included its receipt of discounted services in exchange for access to customer data. Any company that has entered into a similar arrangement with a third-party analytics or advertising partner should inform its users of the "sale" of their data and be prepared to process its customers' opt-out requests including those taking the form of a Global Privacy Control signal.

On Jan. 1, 2023, the California Privacy Rights Act (CPRA) is set to go into effect. The CPRA amends the CCPA to, among other things, remove the 30-day cure period currently provided to correct non-compliance. Companies

continued on next page

should take proactive steps to ensure their compliance with California's consumer privacy laws, as robust enforcement is expected to continue into 2023 without the safety of the 30-day grace period to correct certain non-compliance.

[1] In addition to the $1.2 million fine, Sephora has agreed to provide notice to its customers about the sale of their personal information and provide the required means of opt-out, including through GPC. Sephora has further agreed to conform all service agreements to CCPA requirements and to implement a fulsome CCPA compliance program which is required to deliver an annual report to the AG's office.

For more information, contact:

Peter Bogdasarian
Partner
202.419.8405 | pbogdasarian@stradley.com

Sara P. Crovitz
Partner
202.507.6414 | scrovitz@stradley.com

Mischa S. Wheat, CIPP/US
Associate
215.564.8597 | mwheat@stradley.com