Kilpatrick

SEPTEMBER 1, 2022

CCPA Financial Penalties: Four Takeaways from the California AG's $1.2 Million Enforcement Action that Should Inform Your Compliance Strategy

by Vita E. Zeltser

We warned you last summer that California Consumer Privacy Act ("CCPA") enforcement was heating up! The California Attorney General ("CAG") announced a settlement with cosmetics retailer, Sephora. That, among other penalties, requires Sephora to pay a $1.2 million fine. The enforcement action and settlement was primarily based on Sephora's failure to post a "Do Not Sell My Info" link, respond to browser-level opt out Global Privacy Control ("GPC") signals, and adequately describe the relevant selling of data in its privacy policy.

This action by the CAG gives some insight into the future of CCPA enforcement, even as the law is set for a statutory and regulatory update next year. The CAG's press release summarizing the settlement is available here.

1. CAG Enforcement Set to Continue.

Although California's new privacy agency, the California Privacy Protection Agency ("CPPA"), has CCPA enforcement authority, the CAG appears determined to continue enforcing the law, per its statutory authority to do so. Signaling only that enforcement may ramp up, the CAG reiterated that "[t]here are no more excuses" for a business's failure to comply with the law (despite materially changing and unsettled regulations). Given the discussions of a potential federal law that would preempt most of the CCPA, the CAG was also likely sending a signal that a vigorously enforced California privacy law has value and should not be replaced.

Businesses should be alarmed by CAG's treatment of the CCPA's notice and cure period, pursuant to which businesses have 30 days to cure alleged CCPA violations. The notice and cure period becomes optional beginning in January 2023, and the CAG highlighted the cure period expiration in its press release on the Sephora settlement, likely signaling that the CAG will opt to not provide such a cure period starting next year.

2. Responding to the GPC is Mandatory.

The settlement underscores the CAG's opinion that responding to the GPC as a request to opt out of "sales" is a mandatory aspect of complying with the CCPA. The CAG claimed that user-enabled privacy controls are a "game changer for consumers" and that businesses must process them as opt-out requests. That advice, significantly, seems to align with the CPPA's understanding that responding to the GPC does not become optional when the California Consumer Privacy Rights Act (the "CPRA") amends the CCPA next year. Businesses (and, as applicable, their privacy vendors) must immediately operationalize treating the GPC as a request to opt out of selling, at least at a browser level.

3. The CAG's Priorities Remain Consistent.

The CAG's enforcement priorities do not seem to have changed since last summer. Along with the settlement announcement, the CAG released information about a sweep of loyalty programs (available here) and new enforcement case examples (available here). Loyalty programs, which may constitute a "financial incentive" under the CCPA, and consumers' right to opt-out of "sales" have long been a particular focus of the CAG since last summer.

The CAG may focus on financial incentives based on a belief that personal information collected through those programs is more valuable than the corresponding discounts offered to consumers. Businesses with loyalty programs should mitigate that risk by disclosing, with at least reasonable detail, that any discounts offered to consumers under a loyalty program are proportionate to any value obtained by businesses from collecting the consumers' personal information.

In light of the CAG's activity, businesses would be well-advised to review their websites and online trackers for CCPA compliance. The CAG and CPPA continue to promulgate regulations and bring enforcement actions regarding consumers' right to opt out of sales in the context of online advertising/tracking. Such a focus is interesting for a few reasons. First, the CAG's very broad interpretation of "selling" seems to make the forthcoming right for consumers to opt-out of "sharing" (sharing for cross-contextual advertising purposes) essentially obsolete. Second, the CCPA's concept of "selling" is not confined to online tracking, but the CAG has a much easier time checking a website to see if "online" selling occurs rather than gathering information on a company's backend information flows (i.e., "offline" selling). Third, many companies rely on service provider relationships to take (at least some) online tracking outside of the scope of "sales," whereas the CAG complaint notes that Sephora did not have "valid" service provider agreements in place. As customers of online tracking technology are often forced to sign the provider's paper, consider reviewing those agreements for CCPA service provider requirements following the Sephora settlement.

4. Draft Your Privacy Policy as if the CAG Will Read It.

The CAG is reading your privacy policy, so draft accordingly. The Sephora allegation contains detailed descriptions of Sephora's privacy policy - and not just the plain text of the policy, but also how a user navigates with the policy. The CAG's recent enforcement action summaries also tend to include notes about errors in the relevant business's privacy policy. Taken together, businesses should ensure that (i) their privacy policies strictly comply with detailed substantive requirements set out in the regulations and (ii) navigating within a policy is a seamless user experience (e.g., no broken or circular links). California continues to lead the way in U.S. privacy law, so it is critical to review your existing privacy program to make sure it's prepared for additional regulatory scrutiny.