



Subscribe to Our Newsletter

Enter your email

Subscribe



ROB BONTA

Attorney General

CCPA Enforcement Case Examples

The Office of the Attorney General (OAG) is responsible for enforcing the CCPA. The OAG began sending notices of alleged noncompliance to companies on July 1, 2020, the first day CCPA enforcement began. Once a company is notified of alleged noncompliance, it has 30 days to cure that noncompliance. This may require more than just starting to comply with the law. Overall, curative actions have strengthened consumers' privacy protections. **As of January 1, 2023, the CCPA no longer requires notice of a violation or an opportunity to cure before filing an enforcement action.**

As a law enforcement agency, the OAG does not generally release information to the public about its investigations. The OAG provides the information below as illustrative examples of situations in which it sent a notice of alleged noncompliance and steps taken by each company in response. Please note that the information below does not include all the facts of each situation and does not constitute legal advice.

Updated 08/24/2022

Online Retailers Implemented Opt Out Procedures, Including GPC

Industry: Consumer Retail

Issue: Failure to honor consumer opt outs of sales

In an enforcement sweep, multiple online retailers were found to be using web tracking technologies to make consumers' personal information available to third parties in exchange for services like advertising or analytics, without offering an opt-out mechanism or ensuring the third party was a CCPA-compliant service provider. Specifically, these retailers did not process a consumer's request to opt-out via a user-enabled global privacy control, as required by the CCPA regulations. After being notified of alleged noncompliance, these businesses reviewed and updated service-provider contracts, implemented technology to communicate a "restricted use" signal to third-party recipients of personal information, and blocked some transfers of personal information upon detection of the Global Privacy Control (GPC).

Loyalty Programs Posted Notices of Financial Incentives That Disclosed Material Terms and Obtained Opt-In Consent

Industry: Retail including clothing, home goods, and household staples; Food and beverage; Hospitality; and Home improvement.

Issue: Noncompliant Notice of Financial Incentive

In an enforcement sweep, multiple businesses were found to be operating loyalty programs that offered financial incentives (including product discounts, service differences and/or reduced prices) for the collection of consumers' personal information without posting a compliant Notice of Financial Incentive. The businesses were notified. In response, and specific to the alleged violations, businesses respectively:

- Posted a Notice of Financial Incentive at cash registers where consumers would reasonably encounter the terms before voluntarily joining the loyalty program;
- Revised online interfaces to clearly direct consumers to the Notice of Financial Incentive via an appropriately titled "deep link";
- Redesigned their loyalty programs' enrollment methods to capture express opt-in consent and to meaningfully provide consumers with the right to withdraw from the program at any time; and/or
- Revised their Notices of Financial Incentives to provide consumers with the material terms of the financial incentive. Material terms include the business's use of consumer personal information collected as part of the financial incentive, such as for the purpose of sale, consumer profiling, or to personalize offers and other marketing.

Weblink Shortener Updated Privacy Policy and Added Request Methods

Industry: Technology

Issue: Non-Compliant Privacy Policy and No Request Methods

A business that provides weblink abbreviation tools did not provide notice of the required CCPA consumer rights, including the right to know, delete, and to not be discriminated against, nor did it disclose the request methods established for consumers to exercise their CCPA rights. The business also did not explicitly state whether or not it had sold personal information and did not provide a clear and conspicuous "Do Not Sell My Personal Information" link. After being notified of alleged noncompliance, the business updated its privacy policy to include the required CCPA rights, implemented two request methods, and added a compliant opt-out link.
