ALERT MEMORANDUM

CCPA Regulations Finalized, Enforcement Set to Begin July 1st

June 11, 2020

On June 1, 2020, almost two years since the enactment of the California Consumer Privacy Act (the "CCPA"), and one month before its enforcement is set to begin, the California Attorney General has released the final set of regulations for the CCPA's implementation (the "Regulations"). (We previously analyzed the CCPA here, the legislative amendments here, the Initial Regulations here, the February Revisions to the Regulations here, and the March Revisions to the Regulations here). The CCPA requires covered businesses (broadly defined to include most for-profit entities with over $25 million in annual gross revenue which collect personal information of California residents)[1] to comply with requirements that give California consumers rights to know what personal information has been collected about them, the sources of the information, the purpose of its collection, and whether it is sold or otherwise disclosed to third parties. It also gives consumers certain additional rights, including the right to access personal information about them held by covered businesses, to require deletion of the information and/or to prevent its sale to third parties. Upon approval by the Office of Administrative Law (the "OAL"), businesses will have definitive regulations to follow in their efforts to comply with the CCPA before the Attorney General begins enforcing the law on July 1, 2020.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

WASHINGTON

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

Below we highlight key elements of the Regulations material to businesses in finalizing policies and procedures related to their compliance with the CCPA's requirements:

[1] Businesses that are covered are for-profit entities, located anywhere in the world, that do business in California, collect (or engage a third party to collect) the personal information of California residents and satisfy at least one of the following: (i) have over $25 million in annual gross revenue; (ii) buy, sell, or receive or share for commercial purposes, the personal information of 50,000 or more California residents, households or devices (households and devices are not limited to those in California or owned by California residents); or (iii) derive 50 percent or more of their revenue from the sale of personal information of California residents (any such entity a "covered business"). It also applies to any parent or subsidiary of a covered business that uses the same branding.

Required Communication to Consumers

The CCPA requires covered businesses to provide consumers with a notice of collection at or before the point of collection of personal information, as well as maintaining a privacy policy containing specific information set forth in the Regulations. Additionally, if a covered business sells personal information of consumers, it must provide a notice of the right to opt-out of sale. The Regulations require both notices and the privacy policy to be: (i) written in plain, straightforward language, avoiding technical and legal jargon; (ii) available in languages in which the business in its ordinary course provides information to California consumers; and (iii) accessible to consumers with disabilities.

Notice at Collection.

Notice Presentation. The Regulations provide that the notice at collection should be presented in a manner consistent with the nature of the interaction with consumers and use a format that draws the consumer's attention. The Regulations provide examples of acceptable places to provide such notices at collection; e.g., a business that collects personal information from a consumer online may provide a link to an online notice (or to the business's privacy policy that contains the requisite information) on the introductory page of the website and on all webpages where personal information is collected; a link to the notice for mobile applications on the download page and within the application; and printed notices at the physical point of offline collection or prominent signage directing consumers to where the notice can be found online.

Notice Content. The Regulations require that the notice at collection include: (i) the categories of personal information collected by the business; (ii) the business or commercial purpose for which such information shall be used; (iii) unless the business does not sell personal information and states in its privacy policy that it does not sell personal information, a link titled "Do Not Sell My Personal Information" or, in the case of offline notices, directing the consumer to where such a webpage may be found online (as discussed further below); and (iv) a link to the business's privacy policy, or, in the case of offline notices, directions indicating where such a policy can be found online.

Privacy Policies.

Privacy Policy Presentation. Under the Regulations, a business's privacy policy must provide a comprehensive description of its **online and offline** practices regarding the collection, use, disclosure and sale of personal information, and the rights of the consumer related to their personal information. The privacy policy must be made available to consumers in a format that allows it to be printed as a document, and may be posted online through a conspicuous link containing the word "privacy" and must be available on the business's website homepage, or the download or landing page of a mobile application. If a business does not operate a website, then it must make its privacy policy conspicuously available to consumers.

Privacy Policy Content. In order to be CCPA-compliant, a business's privacy policy must include the date the privacy policy was last updated and provide to California consumers the following:

1. A description of:
   (a) the categories of personal information the business **currently collects** about consumers, as well as the categories of personal information the business **has collected** about consumers in the preceding 12 months;
   (b) the categories of sources from which the personal information is collected;
   (c) the business or commercial purpose for collecting or selling personal information;
   (d) the categories of personal information (if any) that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months; and, for each category of personal information identified, the categories of third parties, if any, to whom the information was disclosed or sold;
2. A description of consumers' rights under the CCPA; namely, the rights to: (i) know about the

personal information collected, disclosed or sold; (ii) request deletion of personal information; (iii) opt-out of sale of personal information; and (iv) non-discrimination on the basis of exercising statutory rights;

3. One or more mechanisms to submit a verifiable request to exercise the consumer's rights under the CCPA, including links to any online request form or portal available for making the request; and a general description of the process used by the business to verify a request to exercise rights, with any information the consumer must provide in connection with any such process;

4. Whether or not the business sells personal information and whether the business has actual knowledge that it sells the personal information of minors under the age of 16;

5. Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf; and

6. A point of contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

Right to Opt-Out of Sale of Personal Information

"Do Not Sell My Personal Information" Link.

A business that sells personal information of consumers must provide: (1) a notice at collection of the right to opt-out (including a link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" or, in an offline notice, direction to the webpage containing such a link); and (2) a clear and conspicuous link on the main screen or landing page of the business's website or mobile application titled "Do Not Sell My Personal Information" or "Do Not Sell My Info". Each link must take you to a page which contains the following information: (i) a description of the consumer's right to opt-out of the sale of their personal information by the business, (ii) an interactive form by which the consumer may submit their request to opt-out online, or, if the business does not operate a website, an offline method by which the consumer can submit their request to opt-out, and (iii) instructions for any other method by which the consumer may submit their request to opt-out. Note, that a business may not sell personal information it collected during the time the business did not have a notice of the right to opt-out posted, unless it obtains affirmative authorization from the consumer.

Exercising and Processing Consumers' Right to Opt-Out.

1. *Exercising the Right to Opt-Out.*

   (a) *Submission Mechanism*. A business which sells personal information must provide at least two easy-to-execute mechanisms requiring minimal steps by which consumers can exercise their right to opt out of sale of personal data, including a clear and conspicuous "Do Not Sell My Personal Information" link (and, if applicable, an opt-in consent mechanism for minors) prominently placed on the business's website or mobile application.

   (b) *Timing*. Within **15 business days** of receipt of a request to opt-out, a business must: (i) comply with the request and notify any third parties to whom it sells personal information of the consumer's request, directing them to not sell the requesting consumer's personal information; or (ii) may notify the requester that it will deny the request, along with an explanation of the reason for the denial.

2. *Responding to Requests to opt-out*. When processing requests to opt-out a business must treat user-enabled global privacy controls which clearly communicate or signal an intent to opt-out

of the sale of personal information as requests to opt-out;[2]

3. *Sale Following Opt-out*. Following a request to opt-out, covered businesses must require a two-step opt-in process prior to resuming sale of a consumer's personal information which includes a clear request to opt-in and a separate confirmation of the choice to opt-in.

Consumer Requests to Know and Delete: Verification, Submission and Response

Verification of Consumer Requests.

The Regulations require that a business establish, document and comply with a reasonable and proportionate method for verifying that the person making a request to exercise rights under the CCPA is the consumer about whom the personal information was collected by the business (or their authorized agent), and must implement reasonable security measures to detect and prevent fraudulent activity, unauthorized access to or deletion of a consumer's personal information.

When establishing verification procedures, the Regulations instruct that businesses should consider (i) the type and sensitivity of information collected and maintained about the consumer; (ii) the risk of harm to consumer as a result of unauthorized access or deletion; (iii) the likelihood that a fraudulent or malicious actor would seek such personal information; (iv) whether information provided by consumer in verification process is sufficiently robust to protect against fraud; (v) the manner in which business interacts with consumer; and (vi) the available technology for verification.

The Regulations delineate differing degrees of verification required, based on the type of request the consumer is making, corresponding to the risk of harm to the consumer if an unauthorized request of that nature is fulfilled:

1. *To know categories of information the business collects*. Businesses must verify to a "reasonable degree of certainty", which may include matching at least two data points provided by the consumer with data points maintained by the business which the business has determined to be reliable for verification purposes.
2. *To know specific pieces of information the business collects about the requesting consumer*. Businesses must verify to a "reasonably high degree of certainty"; which may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for verification purposes, together with a signed declaration, under penalty of perjury. If this standard cannot be met, the business may process the request instead as a request to know categories of personal information subject to the "reasonable degree of certainty" standard above.
3. *To delete information*. Businesses must require verification to a "reasonable degree" or "reasonably high degree of certainty" depending on the sensitivity of the personal information and risk of harm to consumer posed by unauthorized deletion.
4. *To opt-out of sale*. Requests to opt-out are not subject to a verification requirement, but may be denied based on a business's good-faith, reasonable and documented belief that the request is fraudulent.

Moreover, the Regulations provide the following general guidelines for businesses with respect to crafting submission and verification procedures:

1. If applicable, use the same authentication methods used to initially receive the data (e.g., a business may satisfy verification requirements if it requires consumers with password-protected online

[2] In its responses to comments, the OAG noted that Global opt-out mechanisms should control in cases where the consumer uses a global opt-out or do not track signal and also gives explicit consent to the business or site in question regarding collection, use, or disclosure of the consumer's personal information.

accounts to make requests through their existing authentication practices for the consumer's account);

2. If applicable, verify a requester's identity by asking questions to determine whether the requester knows information the consumer has already provided to the business;
3. Use personal information collected from consumers in connection with verification of a request solely for purposes of verification, and delete such information after the verification process is complete;
4. Avoid collection of personal data for verification purposes that is more sensitive than the data that they already collect (e.g., do not collect social security numbers, driver's license numbers, account numbers, or credit card information for verification purposes); and
5. Businesses may not charge consumers or their agents for identity verification, nor implement verification mechanisms which are so burdensome that they will discourage exercise of rights granted under the CCPA.

Submission Methods and Responding to Requests to Know or Delete.

The Regulations also provide specific rules and guidance with respect to submission mechanisms and responses to consumer requests based on the right that the consumer seeks to exercise under the CCPA:

1. *Submission of Requests to Know or Delete*. The Regulations relating to methods for submitting requests and the time permitted to respond to such requests are the same for submitting and responding to consumer requests to know or delete information:
   (a) *Submission Mechanism*. A business must offer at least two methods of submission, including at minimum a toll-free telephone number, and should consider its primary method of interaction with consumers in selecting those methods.[3]
   (b) *Two-Step Authentication for Deletion*. A business may implement a two-step process for requests to delete made online, whereby consumers must first submit a verifiable request, and separately confirm that they want their personal information to be deleted. However, a business must require such a confirmation if the identity of the consumer was verified through access to a pre-existing password-protected account.
   (c) *Timing*. Businesses must confirm receipt of the request within **10 business days** and respond to the request within **45 calendar days** from the date the request is received, with a possibility of a one-time, 45-calendar-day extension, for a maximum of 90 calendar days to respond to the request.

The Regulations also provide specific requirements regarding the contents and nature of responses to each type of consumer request, including:

1. *Responding to Requests to Know*. When responding to a request to know, a business must never disclose: (i) certain biometric data; (ii) Social Security Numbers; (iii) driver's license numbers or other government issued ID numbers; (iv) financial account numbers; (v) health insurance or medical ID numbers; (vi) an account password or security questions and answers; but must inform the requesting consumer with sufficient particularity the categories of biometric and other sensitive information collected, as applicable, to provide the consumer with a

[3] For example, businesses which interact with consumers in person should consider implementation of an in-person method (e.g., a printed form, tablet or computer portal, or telephone by which the consumer can submit requests to know in person), and businesses which operate exclusively online (and have a direct relationship with the consumers from whom they collect personal information) are exempt from the two-method requirement and may provide only an email address for submitting requests to know.

meaningful understanding of the collected information.

2. *Responding to Requests to Delete*. When denying a request to delete personal information which it sells, a business must offer the requesting consumer an opportunity to exercise the right to opt-out with respect to such information.

Other Key Compliance Obligations

Training and Record Keeping. In addition to implementing CCPA compliance policies and procedures, businesses must also train employees responsible for handling consumer inquiries about the business's privacy practices or compliance with the CCPA regarding the requirements of the CCPA and Regulations, including how to direct consumers to exercise the rights that are granted therein.

Contracts with Service Providers. The CCPA grants "service providers" and businesses utilizing service providers protection from certain notice requirements, compliance obligations or liability for violations provided the parties are bound to a written agreement containing certain terms specified by the CCPA.[4] Additionally, a covered business should consider contractual provisions to address its compliance obligations under the CCPA, and its service providers' role in responding to requests from consumers under the CCPA. For example, covered businesses might require service providers to: (i) provide reasonable and timely assistance to the business to enable the business to comply with verifiable consumer requests; (ii) maintain reasonable technical, administrative and physical safeguards over personal information; and (iii) notify to the business of any unauthorized access, disclosure or other compromise of the security, confidentiality or integrity of the disclosed personal information. Further, a business should specify how it would like its service providers to respond to consumers requests to know or delete, as the Regulations allow service providers to **either** respond to such requests on behalf of the collecting business or to refer the requesting consumer to the business directly.

Obligations of Service Providers. The CCPA exempts service providers from the reporting and notice obligations of a covered business; however, they must assist the businesses which provide them with personal information in complying with verifiable requests to know or delete. The Regulations also require that a service provider must not:

1. sell personal data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business; or
2. retain, use or disclose personal information obtained in the course of providing services except:
   (a) to process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, in compliance with the written contract for services;
   (b) to retain and employ another service provider as a subcontractor;
   (c) for internal use to build or improve the quality of its services, but not to build or modify profiles to use in providing services to another business, or correcting or augmenting data acquired from another source; or
   (d) to detect security incidents, protect against fraudulent or illegal activity, comply with federal, state or local laws, or civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state or local authorities, cooperate with law enforcement agencies, or make or defend against claims.

[4] The recipient of the data must agree in a written contract to refrain from: (i) selling the personal information; (ii) retaining, using or disclosing the personal information for any purpose (including a commercial purpose) other than performing the services specified in the contract; and (iii) retaining, using or disclosing the personal information outside of the direct business relationship between the recipient and the business.

Non-discrimination and Financial Incentives. Finally, the CCPA requires that businesses not discriminate against consumers who choose to exercise their rights under the CCPA, including through offering financial incentives (including different prices or services) based on the exercise of such rights which either: (i) are not reasonably related to the value of the consumer's data; or (ii) would reasonably affect the ability of the business to perform the services or offer the goods requested by that consumer.

If a business offers financial incentives to consumers in connection with their personal information, it must provide a plain, straightforward notice explaining the material terms of the financial incentive or price or service difference offered, in a reasonably accessible format.

The notice of financial incentive must identify the categories of personal information that are implicated by the financial incentive or price or service difference, how the consumer can opt-in to the financial incentive or price or service difference, the value of the consumer's data, and how the financial incentive or price or service difference is reasonably related to the value of the consumer's data (including a good-faith estimate of the value of the consumer's data, and a description of the method of valuation).

Conclusion

The final Regulations did not resolve all remaining ambiguities under the law, but as enforcement is set to begin on July 1, 2020, businesses should look to the final Regulations to prioritize compliance efforts, if they have not already done so.

…

CLEARY GOTTLIEB