CPPA – California Consumer Privacy Act Proposed Regulations Executive Summary

The California Privacy Protection Agency (CPPA) released a proposed regulations implementing the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA).

BACKGROUND

The CCPA was signed into law on June 28, 2018, becoming effective on January 1, 2020. The statute gave rulemaking and enforcement authority to the California Attorney General. Pursuant to this authority, the CA AG issued regulations that went into effect on August 14, 2020, and subsequently adopted amendments went into effect on March 15, 2021.

California voters later approved the CPRA in November 2020, which established the CPPA to enforce the CCPA. Rulemaking authority was formally transferred from the CA AG to the CPPA on April 21, 2022, and on May 5, 2022, California's Office of Administrative Law formally approved the transfer.

Who Must Comply?

The CCPA/CPRA applies to all industries and to all entities that meet the definition of a "business" under the CCPA/CPRA.

Prior to January 1, 2022. Under CCPA rules, a "business" is defined as doing business in California that collects consumers' personal information, directs how it is used, and meets **one** of three thresholds:

1. Annual adjusted gross revenues over $25 million;
2. Annually buys, receives, sells or shares for commercial purposes, the **personal information of** 50,000 or more consumers, households, or devices; and/or
3. At least 50% of its annual revenues come from selling consumers' personal information.

Any entity that "controls" or is controlled by a "business" and that shares "common branding."

As of January 1, 2022. However, the CPRA changed the scope of covered businesses. Part of the definition of a business is that it satisfies one or more of the following thresholds:

1. As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
2. Alone or in combination, annually buys or sells, or shares the personal information of 100,000 or more consumers or households.
3. Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal Information.

Credit unions and CUSOs that meet the definition of a business will be required to comply with its provisions, but only insofar as they collect "personal information" that exceeds the scope of "personally identifiable financial information" under the California Financial Information Privacy Act (CFIPA) (SB 1; Cal. Fin. Code §4050, et seq.) and the Gramm-Leach-Bliley Act (GLBA) (federal regulations 12 CFR Part 1016).

Notwithstanding, a credit union or CUSO subject to CCPA/CPRA may be liable under CCPA for a data breach with regard to ANY personal information, including information collected under the scope of CFIPA and GLBA.

What is the Effective Date?

The effective date of CPRA is January 1, 2023, but there would be a "look-back" period beginning on January 1, 2022 for access rights.

For ease of reference, a timeline of these dates are as follows:

- **July 1, 2021 –** Agency rulemaking process start date.
- **January 1, 2022 –** Look-back period begins.
- **July 1, 2022 –** Final date for Agency to adopt regulations.
- **January 1, 2023 –** CPRA becomes effective. In addition, the employees and business-to-business (B2B) exemptions sunset, unless otherwise extended.
- **July 1, 2023 –** CPRA enforcement date.

SUMMARY

General Overview

On July 8, 2022, the CPPA began the formal rulemaking process to adopt proposed CCPA regulations implementing CPRA. The proposed regulations:

1. Update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA.
2. Operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law.
3. Reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand.

Key Takeaways

Below, we provide high-level takeaways from the proposed regulations, discuss the rulemaking timeframe, and provide a summary of some of the more notable provisions.

I. ARTICLE 1 – GENERAL PROVISIONS

A. Key Definitions (§7001)

This section introduces a number of new definitions that are outlined in the CPRA that were not included in the CCPA, including:

Key Definitions	
Disproportionate effort	A standard which requires a business to prove that the time and/or resources needed to facilitate a consumer request would be significantly higher than the benefit to the consumer.
First party	Means the consumer-facing business with which the consumer intends and expects to interact. *This definition is likely included to differentiate between the new obligations that apply to "third parties" under the CPRA.*
Frictionless manner	Means a business's processing of an opt-out preference signal that complies with the requirements set forth in Section 7025(f) (noted below).
Opt-out preference signal	Means a signal that is sent by the platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to

	opt-out of the sale or sharing of personal information and complies with the requirements set forth within the draft regulations.
Unstructured data	Means personal information is not organized in a predefined manner, such as text, video files, and audio files. *This definition is relevant because in order to comply with "Requests to Correct" under the law, covered businesses must consider the nature of the personal information (i.e., whether it is objective, subjective, unstructured or sensitive).*

B. Restrictions on Collection and Use of Personal Information (§7002)

A business's collection, use, retention, and/or sharing of a consumer's personal information must be reasonably necessary and proportionate to achieve the purposes for which it was collected or processed.

The draft regulations provide illustrative examples of how this standard should be applied.

C. Requirements for Disclosures and Communications to Consumers (§7003)

The regulations require that any disclosures and communications to consumers be easy to read and understandable to consumers, using plain text and straightforward language and avoiding jargon.

D. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent (§7004)

Under the regulations, businesses would be required to design and implement methods for submitting requests under the California Consumer Privacy Act (CCPA) and CPRA for obtaining consumer consent that incorporates the following principles:

a. **Easy to understand.** Methods must use language that is easy for the consumer to read and understand.
b. **Symmetry in choice.** Businesses that use a simple flow for a consumer to opt into the sale of the data, will also be required to follow the same number of steps in allowing the consumer to opt out of the sale of the data.
c. **Confusing language and manipulation.** Confusing language such as double negatives and manipulative language or bundling consents is prohibited so that (1) the consumer is not confused; and (2) eliminated consumer manipulation or guilts the consumer through bundling consents, does not unnecessarily burden the consumer with untested or broken methods to submit CCPA request.

Of note, the proposed regulations state that methods of obtaining consumer consent that do not comply with the draft regulations' principles may considered "**dark patterns**," and that any agreement obtained through the use of dark patterns does not constitute as consumer consent.

II. ARTICLE 2 – REQUIRED DISCLOSURES TO CONSUMERS

Article 2 addresses required disclosures to consumers. The updates in this Article were originally drafted in response to public comments received by the Attorney General's Office expressing confusion about the number and type of notices that businesses are required to provide.

The following are key highlights from Article 2 that businesses must follow.

A. Overview of Required Disclosures (§7010)

In general, the provisions now extend to businesses that **control** consumers' personal information rather than businesses that **collect** personal information.

Moreover, a business's opt-out notice must cover both the sale and **sharing** of personal information or the alternative opt-out link (described below).

B. Privacy Policy (§7011)

The proposed regulations include a number of modifications to a business's privacy policies. Most notably, the policy must indicate whether the businesses use or disclose sensitive information for purposes other than those specified in §7027, subsection (l) (see Article 3 below).

Additionally, businesses will need to update the consumer rights section in their privacy policy to reflect:

a. **Right to know**. Consumers have a right to know what personal information the business has collected about the consumer.
b. **Right to delete**. Consumers have a right to delete that a business has collected from the consumer (subject to certain exceptions).
c. **Right to correct**. Consumers now have the right to correct inaccurate information that a business maintains about the consumer.
d. **Right to opt out**. The right of consumers to opt out of the sale of their personal information by the business now also reflects a right to opt out of the sharing.
e. **Right to limit**. If the business uses or discloses sensitive personal information for reasons other than those permitted under the law, the consumer has the right to limit the use or disclosure of sensitive personal data by the business; and
f. **Right to nondiscrimination**. The right to nondiscrimination is now explicit and includes the right not to be retaliated against for the exercise of their CCPA rights and includes employees, applicants, and independent contractors.

C. Notice at Collection of Personal Information (§7012)

The proposed regulations include a new notice for third parties that "control the collection" of personal information. For example, when a first party allows a third party to collect personal information from consumers, the first party will need to provide notice and identify the third party as an entity that collects consumer personal information. Additionally, the third party will also need to provide a notice of collection if it is a third party in relation to the information and "controls" the personal information being collected.

D. Notice of Right to Opt-Out of Sale/Sharing and the "Do Not Sell or Share My Personal Information" Link (§7013)

CPRA's amendment extends the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information. For example, clicking on the opt-out link must "either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice."

Links also must be conspicuous. For websites, links must appear in a similar manner as other links used on the business's homepage. For Apps, links must be accessible such as through the settings menu and in the privacy policy.

Finally, businesses do not need to provide a link if they process opt-out preference signals in a "frictionless" manner (see below for more discussion of this issue).

E. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link (§7014)

CPRA adds this section to ensure that notice is easily accessible and understandable and that businesses have clear guidance on how to provide information required for disclosure. Businesses will be

required to include a link to immediately effectuate the consumer's right to limit the collection of sensitive personal information.

F. Alternative Opt-Out Link (§7015)

The purpose of the alternative opt-out link is to ensure uniformity of the alternative opt-out link so that the link is easily accessible and understandable to consumers, including those with disabilities, and to ensure that the link easily allows the consumer to opt out of the sale and sharing of the consumer's personal information to limit the use or disclosure of the consumer's sensitive personal information.

G. Notice of Financial Incentive (§7016)

The Agency clarifies that only price and service differences require a valuation of data. Other kinds of financial incentives where a monetary or specific benefit (e.g., free t-shirt, gift card, etc.) is given for the exchange of data do not require a valuation because the consumer is aware of the value of the good and able to factor it into their decision of whether to provide the personal information.

III. ARTICLE 3 – BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

A. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know (§7020)

The CPRA consolidated the requirements so that they are the same for requests to delete, requests to correct, and request to know. Further, this section has been revised to add that the two-step process to make online requests to delete shall otherwise comply with section 7004. This is necessary to ensure that the two-step process is not implemented in a manner that would subvert the consumer's intention.

B. Requests to Delete (§7022)

The proposed regulations provide new details on how service providers and contractors must respond to a business's notification that a consumer has exercised their right to deletion. For example, they must permanently delete the information and notify their own service providers and contractors to delete the information.

C. Requests to Correct (§7023)

Under CPRA, a consumer has the right to request a business to correct any inaccurate personal information, which the proposed regulations operationalize through §7023.

Upon verification, a business must determine the accuracy of the personal information by considering the totality of the circumstances relating to the contested personal information. The Agency provides some guidance on this analysis such as considering the nature of the personal information, how the business obtained it, and documentation relating to the accuracy of the personal information. Businesses also are permitted to request that consumers provide documentation if necessary. Businesses that correct personal information also must implement measures to ensure the information stays corrected and that service providers and contractors correct it.

D. Requests to Know (§7024)

CPRA expands the period of time covered by consumer right to know requests beyond the 12-month period as provided in CCPA. Under CPRA, a consumer's right to request required information beyond the 12-month window is only applicable to personal information collected on or after January 1, 2022. §7024 operationalizes this provision.

E. Opt-Out Preference Signal (§7025)

The proposed regulations would require a business to process any properly formatted opt-out preference signal as a valid request to opt out of the "sale" of personal information or the "sharing" of personal information for cross-context behavioral advertising.

F. Requests to Opt-Out of Sale/Sharing (§7026)

Proposed regulations state a notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.

Businesses are also required to provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

G. Requests to Limit Use and Disclosure of Sensitive Personal Information (§7027)

A business that uses or discloses sensitive personal information is required to provide at least two methods for exercising this right. As with the right to opt out of sale/sharing, the Agency takes the position that a notification or tools regarding cookies are not, in and of themselves, sufficient. Businesses have 15 business days to comply with the request, which includes notifying service providers, contractors, and third parties.

As with requests to opt-out of sales/sharing, businesses must provide a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and sale of their sensitive personal information.

Finally, the proposed regulations identify seven permissible purposes for processing sensitive personal information without having to provide the right to limit. hose permissible purposes include performing the services or providing the goods that an average consumer would reasonably expect, detecting certain types of security incidents, ensuring for the physical safety of individuals, and for short term transient use.

IV. ARTICLE 4 – SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

The CPRA requires certain contractual provisions between all entities to which a business discloses personal information, including service providers, contractors and third parties. Article 4 of the proposed regulations outlines these specific requirements. This section also outlines a third party's duties to comply with the CPRA with regard to any information it receives from a business pursuant to the law.

A. Service Providers and Contractors (§7050)

The proposed regulations clarifies that a person who contracts with a business to provide cross-contextual behavioral advertising is a third party in relation to the business and not a service provider or contractor. This is an important clarification because all businesses that engage in cross-contextual behavioral advertising will be required to provide consumers with the ability to opt out of the sale or sharing of their information.

B. Contract Requirements for Service Providers and Contractors (§7051)

Section 7051 identifies the requirements for service provider and contractor contracts. The enumerated requirements amount to terms that must be included in such written agreements and functionally extends such requirements to written agreements with subcontractors for service providers and contractors. This section also explicitly states that a person who does not have a contract that complies with these

requirements is not a service provider or a contractor—requiring a compliant agreement to define roles under the CPRA.

The proposed regulations also create a new due diligence stating that whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

C. Third Parties (§7052)

Section 7052 outlines third-party obligations, including the requirement that third parties honor and comply with consumer requests for deletion, opt-out of sale/sharing, and limitation.

D. Contract Requirements for Third Parties (§7053)

The CPRA requires a business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party for a business purpose to enter an agreement with the third party that includes certain provisions. The purpose of section 7053 is to clearly set forth all the provisions that must be included in third party contract with the business, to explain the consequence if the provisions are not included in the contract, and to clarify the duties of the third party and the business as it relates to the contract.

Section 7053 also creates a new due diligence duty in the same manner as the service provider and contractor obligations.

V. ARTICLE 9 – INVESTIGATIONS AND ENFORCEMENT

A. Sworn Complaints Filed with the Agency (§7300)

The CPRA allows individuals and businesses to file sworn complaints against businesses they believe to be in violation of the law. The proposed regulations outline the procedures for how a person can make such complaints, including the information they must submit to the agency.

B. Agency Initiated Investigations (§7301)

Section 7301 provides that all matters that do not result from a sworn complaint may be opened on the Agency's initiative.

C. Probable Cause Hearings (§7302)

The CPRA allows the CPPA to conduct probable cause hearings when evidence supports a reasonable belief that the CPRA has been violated. The proposed regulations outline the procedures that the CPPA must follow to conduct these hearings.

D. Stipulated Orders (§7303)

The proposed regulations permit the CPPA to enter into a stipulated order with a person who is under investigation (in lieu of an administrative hearing). The stipulated order has the force of any other order issued by the CPPA.

E. Agency Audits (§7304)

The proposed regulations would allow the CPPA to perform audits in three situations:

1. To investigate possible violations of the CCPA;
2. If the subject's collection or processing activities present significant risk to consumer privacy or security; and
3. If the subject has a history of noncompliance with the CCPA or any other privacy protection law.

These audits may be announced or unannounced, and a business' failure to cooperate with an audit could lead to enforcement action against that business.

COMMENT PERIOD DEADLINE

- August 23, 2022 at 5:00 pm PT

RESOURCES

- **Notice of Proposed Rulemaking**
- **Text of Proposed Regulations**
- **Initial Statement of Reasons**
- **California Consumer Privacy Act of 2018; Cal. Civil Code §§1798.100-1798.199**

QUESTIONS TO CONSIDER

a. The CCPA/CPRA define "business." Credit unions and CUSOs that meet the definition of a business are required to comply with its provisions, but only insofar as they collect "personal information" that exceeds the scope of "personally identifiable financial information" under the California Financial Information Privacy Act (CFIPA) and the Gramm-Leach-Bliley Act (GLBA). They also will be liable under CCPA/CPRA for a data breach with regard to ANY personal information. The regulations do not include nor clarify the CCPA's/CPRA's definition of a "business."

   Would it be helpful for the regulations to include the definition of "business"? Why or why not?

   Is further clarification needed on the definition of a "business"? If so, how should the definition be clarified in the regulations?

b. Despite statutory language suggesting a business can choose whether to accept global opt-out preference signals or provide links to other opt-out mechanisms, the proposed CCPA regulations would require a business to process any properly formatted opt-out preference signal as a valid request to opt out of the "sale" of personal information or the "sharing" of personal information for cross-context behavioral advertising.

   What compliance, technology, or other challenges would your credit union face in implementing such a requirement?

c. The CPPA has the authority to audit a business to ensure the business is within compliance with any provision of the CCPA. However, the proposed regulations are vague on the details regarding the audit process.

   Is clarification needed regarding the audit process? Why or why not?

d. Absent clarification, credit unions may be subject to the CCPA/CPRA, and therefore to audits performed by the CPPA, and CPPA's enforcement authority could extend to both state and federally chartered credit unions. As financial institutions, credit unions are already among one of the most highly regulated industries and currently undergo robust examinations by their

regulatory agencies, which includes their compliance with a plethora of privacy and data security laws and regulations.

Do you believe that credit unions should be exempted from the audit process, or at minimum, should the CPPA coordinate with a credit union's state and federal primary regulators?

e. Several notices and responses are required under the CCPA. The proposed regulations provide guidance on the notices, but do not provide model language or form notices.

Should the regulations provide model notices for compliance with notice requirements? Why or why not? If so, in addition to model notices what other safe harbor provisions would be beneficial?

f. What other concerns or suggestions do you have to improve the proposed implementing regulations?