January 15, 2025

California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear California Privacy Protection Agency,

I write on behalf of the American Financial Services Association (AFSA)[1] and the California Financial Services Association (CFSA) to express the strong concerns of our members regarding the proposed regulations for updates to the California Consumer Privacy Act (CCPA), including provisions related to cybersecurity audits, risk assessments, automated decision-making technology (ADMT), and behavioral advertising. We appreciate the CPPA's continued efforts to enhance consumer privacy while fostering innovation and supporting businesses. However, we believe several aspects of the proposed regulations require refinement to ensure practicality, legal compliance, and alignment with statutory authority.

Cybersecurity Audit Regulations

The proposed cybersecurity audit regulations exceed the CPPA's statutory authority as outlined in Section 1798.185(14)(A) of the CCPA. The CPPA's role should be limited to requiring businesses to conduct annual cybersecurity audits, defining the general scope of such audits, and ensuring that they are thorough and independent. The regulations should avoid imposing specific security processes on businesses. Moreover, the CPPA should allow businesses to comply with equivalent legal and industry standards, such as those outlined in federal or international frameworks, to satisfy the annual audit requirement.

Certain provisions, such as Section 7122(a), conflict with federal guidelines regarding auditor independence and reporting structures. Requirements like mandatory board oversight of auditors, employee training after every data breach, and other prescriptive rules are overly rigid and fail to consider the existing requirements for federally regulated financial institutions. A more flexible approach aligned with federal standards is recommended.

[1] Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including traditional installment loans, direct and indirect vehicle financing, mortgages, and payment cards. AFSA members include national banks and non-bank state licensed financial institutions. AFSA does not represent payday lenders, title lenders, or credit unions.

Section 7123(b)(2) improperly uses the audit framework to impose new cybersecurity requirements, which are not authorized by the CCPA. The law mandates only "reasonable security procedures and practices" under separate statutory provisions and does not empower the CPPA to establish comprehensive cybersecurity mandates. Additionally, Section 1798.81.5 of the California Civil Code already governs information security for certain businesses, exempting federally regulated financial institutions. The CPPA has no authority to regulate under this section.

Provisions in Sections 7123(d)-(e) requiring national banks to report data breaches to state regulators infringe on federal visitorial rights, which limit state authority over national banks. Such disclosures could also expose sensitive information, increasing cybersecurity risks with little benefit.

Finally, while Section 7123(f) acknowledges that duplicative audits are unnecessary, it still demands businesses document compliance in extensive detail. This effectively duplicates efforts for federally regulated institutions already subject to comprehensive audit requirements. To avoid redundancy, the CPPA should exempt businesses meeting federal audit standards from additional state-specific requirements.

Risk Assessment Regulations

The proposed risk assessment regulations should be aligned with existing standards and requirements applicable to federally regulated financial institutions. Harmonization with frameworks like NIST and international standards would ensure consistency and reduce redundant obligations. The statutory mandate for risk assessments explicitly protects businesses from being required to divulge trade secrets. However, this principle is missing from the proposed regulations. To address this omission, the regulations must include explicit provisions that protect trade secrets and intellectual property from disclosure during compliance. Additionally, the confidentiality of all materials submitted to the CPPA should be explicitly safeguarded.

The statute specifies that risk assessments are only required for processing activities presenting "significant risk to consumers' privacy or security." Despite this, the proposed regulations define "significant risk" inconsistently across risk assessments and cybersecurity audits. A single, cohesive standard must be adopted to prevent confusion and overreach. The definition of "significant risk" in Section 7150(b)(3) is excessively broad, as it applies to any "significant decision" using automated decision-making technology. This focus on technology, rather than the processes or risks involved, is inappropriate. If the Agency insists on including "significant decisions," the definition should mirror the GDPR's concept of decisions with "legal or similarly significant effects" to better align with established standards.

Provisions such as Section 7152(a)(5)(I), which require businesses to evaluate subjective psychological harms like stress and embarrassment, are impractical. Assessing such factors falls outside the expertise of businesses and is better left to mental health professionals. Similarly, Section 7152(a)(9), which mandates the identification of a single decision-maker responsible for approving risk assessments, is unrealistic for large organizations. Decisions in such organizations are typically collaborative and cross-functional, making this requirement unrealistic.

Section 7154 uses the statutory mandate for risk assessments to introduce new obligations for businesses to implement corrective actions or modify policies, which goes beyond the statutory authority. The purpose of risk assessments is to evaluate risks versus benefits—not to prohibit or require changes to "risky" processing activities. Section 7154 and related provisions should therefore be removed.

The exceedingly broad triggers for requiring risk assessments, including retroactive application to all existing processing activities, will impose significant operational burdens. The proposed 24-month deadline for completing these assessments exacerbates the issue. The CPPA should limit the application of these requirements to future activities to avoid debilitating effects on businesses.

Finally, the regulations must recognize that many businesses, particularly financial institutions, already comply with extensive risk assessment requirements under federal frameworks. An explicit exemption for federally regulated entities should be included, allowing existing compliance efforts to satisfy CPPA requirements.

Automated Decision-Making Technology (ADMT) Regulations

The definition of automated decision-making technology (ADMT) in Section 7001(f) is overly broad and requires revision. A more appropriate definition would align with the EU GDPR and other U.S. state privacy laws, limiting ADMT to fully automated processes (with no direct human involvement) that utilize personal information to make decisions with legal or similarly significant effects on consumers. These effects should specifically include critical areas such as financial or lending services, housing, insurance, education, criminal justice, employment, healthcare, or access to basic necessities.

Additionally, the interplay between the ADMT and Behavioral Advertising definitions, along with opt-out right provisions, improperly expands opt-out rights to include first-party contextual advertising. This exceeds the CCPA's statutory scope, which is explicitly limited to cross-context behavioral advertising.

Section 7221(b)(2) adds unnecessary complexity by attempting to incorporate human participation into the opt-out paradigm for significant decisions. Instead, the definition of "significant decision" should be revised to match the GDPR standard, which focuses on

decisions involving both human intervention and legal or similarly significant effects. This approach simplifies compliance while staying within statutory authority.

Lastly, Section 7221(g), which requires businesses to explain why a consumer request is deemed fraudulent, should be removed. This provision risks inadvertently assisting fraudsters by revealing the criteria and methods businesses use to detect fraudulent activity, thus enabling future fraud attempts.

Amendments to Existing Regulations

Several proposed amendments impose excessive compliance burdens on businesses without providing meaningful additional protections to consumers. For example, changes in Sections 7023(c), 7023(f)(3), 7023(i), and 7023(j) would require metadata tagging at the individual data element level, an approach that is both costly and operationally burdensome. Existing regulations already ensure sufficient understanding and coordination of data processing, making these granular requirements unnecessary.

The definition of "artificial intelligence" in Section 7001(c) is overly broad and includes non-AI technologies that infer outputs from inputs. This definition is unnecessary to implement the CCPA and lacks statutory support. If retained, the definition should align with industry standards, such as the NIST definition, to avoid including unrelated technologies.

Section 7001(ccc) inappropriately includes minors' (under 16) personal information (PI) within the definition of Sensitive Personal Information (SPI). Similar legislative efforts were vetoed by the Governor, and regulatory amendments should not attempt to circumvent these decisions. Such changes should be pursued through legislation.

The revised language in Section 7003(c), replacing "its homepage(s)" with "any internet webpage where personal information is collected," introduces unnecessary font and typeface requirements that are nonsensical. The original language sufficiently addresses concerns about link visibility and should be reinstated.

Proposed changes to Section 7020(e) extend consumer rights to request information beyond the statutory look-back period of January 1, 2022, conflicting with the statute. Businesses should not be required to provide information they no longer maintain due to standard retention policies. Compliance should be limited to data that is both collected and currently maintained.

The change in Section 7022(f), requiring businesses to ensure external sources do not provide information subject to a deletion request, exceeds statutory authority. The right to delete only applies to personal information collected directly from the consumer, not from third parties.

Sections 7023(c), 7023(f)(3), 7023(i), and 7023(j) impose unrealistic data management obligations, such as ensuring corrected information remains accurate or tracking individual data elements for contested status or source information. These requirements exceed statutory intent, add substantial costs, and offer minimal consumer benefit.

Similarly, Section 7023(k) mandates businesses to ensure corrected data remains accurate indefinitely, which goes beyond the statutory requirement of using "commercially reasonable efforts." Consumers already have mechanisms to verify and correct their data, such as through requests to know and privacy policy disclosures.

Section 7024(d)(2) introduces redundant obligations by requiring businesses to provide a way for consumers to confirm that maintained personal information matches their records. The existing right to know and right to correct sufficiently address this need without adding unnecessary compliance burdens.

Changes to Section 7051, which frequently alter requirements for Service Provider/Contractor Addendum templates, create operational inefficiencies. Businesses must update existing contracts and educate contractors on new language, an effort that can take months or longer for large organizations with extensive relationships. These constant changes offer little improvement in consumer privacy protection and should be reconsidered.

Conclusion

While we recognize the potential for constructive dialogue surrounding these draft regulations, we strongly believe there are critical issues that need to be addressed. The scope of the proposed regulations, particularly with regard to cybersecurity programs, risk assessments, and definitions such as ADMT and behavioral advertising, appears to exceed statutory limits. These issues, along with the impracticality of compliance with several provisions, warrant careful reconsideration. We emphasize the need for more reasonable, targeted definitions and an appropriate timeline for compliance. Additionally, we urge the CPPA to consider alternative compliance pathways that are in line with industry standards. Ultimately, these revisions are necessary to ensure that the regulations do not impose undue burdens on businesses and align more closely with the statutory intent.

Thank you for considering our comments and questions. If you have any questions or would like to discuss this further, please do not hesitate to contact us.

Sincerely,

Elora Rayhan
State Government Affairs
American Financial Services Association
1750 H Street, NW, Suite 650
Washington, DC 20006-5517
erayhan@afsamail.org

Dave Knight
Executive Director
California Financial Services Association
2718 Wrendale Way
Sacramento, CA 95821
(916) 616-7570
dcknight@aol.com