June 2, 2025

Submitted via email: regulations@cppa.ca.gov

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 CPPA Board Members,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to respond to the modifications to the *Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology, and Insurance Companies* published by the California Privacy Protection Agency ("CPPA") on May 9, 2025 (the "Proposed Regulations"). SIFMA appreciates many of the modifications the CPPA has made to the original proposal and urges the CPPA to make additional changes to the Proposed Regulations as outlined below to ensure better harmonization with overlapping federal, state, and non-US laws and regulations applicable to SIFMA members.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets, including a significant presence in California. SIFMA has 20 broker-dealer members headquartered in California. There are approximately 358 broker-dealer main offices, nearly 40,000 financial advisers, and over 100,000 securities industry jobs in California.[2]

[1] The Securities Industry and Financial Markets Association (SIFMA) is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

[2] See SIFMA California Data here https://states.sifma.org/#state/ca

1. **The Proposed Regulations should expressly exempt federally regulated financial institutions from the requirements.**

As a threshold matter, SIFMA continues to recommend that the CPPA expressly exempt federally regulated financial institutions including broker-dealers, registered investment advisers, and banking organizations, as well as their holding companies and affiliates, from the cybersecurity audit, risk assessment, and automated decisionmaking technology ("ADMT") requirements in the Proposed Regulations. As federally regulated financial institutions, SIFMA members are subject to, and have built robust programs adhering to, federal regulatory regimes which cover cybersecurity, risk management, and the use of ("ADMT"). SIFMA members are governed by the Gramm-Leach-Bliley Act ("GLBA") and its regulations that cover cybersecurity, privacy and data protection. SIFMA members are further subject to a plethora of federal financial regulatory frameworks and guidance that govern cybersecurity risk for registrants as well as non-U.S. regulators.[3] Federal regulators require extensive policies and procedures, risk management, reporting and testing under their various regulatory regimes including Reg S-P and the Safeguards Rule. Further, SIFMA members are subject to robust oversight including examinations and enforcement by federal regulators.

Without a clear exemption, financial institutions will be forced to divert resources away from proactively guarding against emergent threats to meet the duplicative and unnecessarily prescriptive regulatory obligations, while also still complying with rigorous federal requirements specifically targeted at the financial services industry.

2. **The Proposed Regulations do not exempt activities that are essential for financial institutions to combat malicious activity.**

SIFMA appreciates the narrowing of the scope of the ADMT requirements in the Proposed Regulations which will help to minimize the risk that the Proposed Regulations would cover longstanding compliance and business use cases. Although most data SIFMA members process is covered by GLBA and therefore exempt from the CCPA and the Proposed Regulations, additional clarification is necessary to ensure that our members' fraud prevention capabilities are not limited by the Proposed Rules. In fact, the Proposed Rules impose more limitations on a covered institution's ability to use ADMT for fraud detection purposes than the previous version despite broad support for such usage in many comment letters.

The Proposed Rules should be further revised to include an explicit exception for fraud detection activities including but not limited to technology used to detect money-laundering, exploitation of seniors, violations of the Foreign Corrupt Practices Act, Ponzi schemes, insider trading, pump and dump schemes and more. Such uses clearly benefit customers and the

[3] Financial regulatory regimes which include data, privacy, and or cybersecurity requirements include those under the Securities and Exchange Commission ("SEC"), Financial Industry Regulatory Authority ("FINRA"), the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission ("CFTC"), the Consumer Financial Protection Bureau ("CFPB"), the Federal Deposit Insurance Corporation ("FDIC"), the National Credit Union Administration ("NCUA"), the U.S. Department of the Treasury,

financial system. As currently drafted, such detection technology is covered thus creating limitations which may not be as beneficial for efficient detection.

Additionally, if an individual decides to opt-out, it can have significant impact on the overall algorithm and models used to detect fraud and provide fraudsters with an additional way to engage in bad activity by opting-out to remain off the radar. The exemption should also specifically allow the use of fraudsters' data for training ADMT models which will help to prevent and catch future frauds. There is no compelling justification for protecting malicious activities or actors, and such data is necessary for training models over time and maintaining the most current defense mechanisms as scams evolve.

Further, there should be a clear exemption for any legal and compliance-related activities which protect customers, investors, the firm, or the financial markets more broadly. Excluding such uses severely impedes the evolution of more efficient compliance systems which runs counter to the goals of the CCPA.

3. The required risk assessments are triggered at an unnecessarily low threshold and are overly prescriptive.

The modified Proposed Regulations do not adequately address the unnecessarily low threshold and the prescriptive nature of the required risk assessments which provide limited benefit to consumers. The threshold does not align with other existing risk assessment frameworks, nor does it align with the other sections of the Proposed Regulations. SIFMA urges the CPPA to adopt a standard that would require a risk assessment for activities that are "likely to result in a high risk to the rights and freedoms of natural persons" as is similarly required under the EU General Data Protection Regulation. Such a standard would more directly benefit consumers as it is directly related to higher risk activities. This would also align with the CPPA's changes to the scope of the ADMT requirements in this version which now apply to "significant decisions." The CPPA should similarly align the risk assessment threshold.

4. The cybersecurity audits are not aligned with existing well-established cybersecurity frameworks and are overly prescriptive.

SIFMA appreciates the significant changes made to the cybersecurity audit requirements in the Proposed Regulations. Aligning the requirements to existing standards is critical for ensuring that work is not duplicated unnecessarily. Unfortunately, the Proposed Regulations do not adequately incorporate those requirements and even contradict existing standards. For example, the Proposed Regulations require a single annual information security audit. The goal of the proposal would be better achieved if the standard were to align with risk assessments based on broader risk assessment standards which may require audit resources to be deployed in higher risk areas as necessary. If warranted, multiple periodic audits should satisfy the requirements of the Proposed Regulations.

The cybersecurity audit requirements also remain overly prescriptive without any clear reason or consumer benefit. For example, the reporting requirements for the internal auditor are unnecessarily restrictive and do not match how many federally regulated financial institutions are organized. The previous version of the Proposed Rules requiring the senior auditor to report to the company's board more accurately reflected how financial institutions are structured but also may not work for other industries. This is a clear example of how unnecessarily prescriptive requirements impose burdens which contradict the purpose of the rulemaking and the CCPA. The Proposed Regulations should be revised to provide more flexibility for firms to meet the cybersecurity audit requirements or clearly exempt federally regulated financial institutions from these provisions.

* * * * *

SIFMA and its members appreciate the opportunity to provide these comments and welcome further discussion. Please reach out to Melissa MacGregor at mmacgregor@sifma.org with any questions or to schedule a meeting.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Kim Chamberlain, Managing Director, State Government Affairs, SIFMA