February 11, 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: Updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology, and Insurance Companies.

Dear CPPA Board Members,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to respond 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 November 22, 2024 (the "Proposed Regulations"). SIFMA values the extensive consultation between the CPPA and the business community to date, but we believe that additional work should be done to better harmonize these requirements with existing U.S. and international standards.

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

Executive Summary

SIFMA recommends that the CPPA make the following changes to the Proposed Regulations:

- Federally regulated financial institutions, including broker-dealers, investment advisers and their representatives, that are subject to a federal financial regulatory regime should be expressly exempt from the requirements in the Proposed Regulations. Financial institutions are already subject to robust cybersecurity, data protection, risk management, and other protocols as well as the vigorous examination and enforcement authority of federal financial regulators. Exempting them from the Proposed Regulations aligns with the spirit of the CCPA.

- The Proposed Regulations should be tailored to match the intended scope of the CPPA's legislative authority and legislative intent of the CCPA. As written, the rules stretch far beyond what the CCPA imposed or anticipated.

- The reporting requirements in the Proposed Regulations should undergo a more rigorous cost-benefit analysis to determine whether the costs of the Proposed Regulations outweigh their purported benefits. The processing thresholds that trigger the requirements should also be increased to cover businesses that process (1) the personal information of 500,000 or more consumers or households, or (2) the sensitive personal information of 250,000 or more consumers.

- The cybersecurity audit requirements should be amended to recognize existing cybersecurity frameworks to reduce conflict and increase efficiency. As such, audit requirements should be risk-based without prescriptive requirements which may detract from a firm's ability to address riskier scenarios.

- The proposed risk assessment requirements, which apply retroactively to ANY existing processing activity and mandate completion of such assessments within 24 months, will impose an incalculable burden upon businesses, resulting in a debilitating impact on their operations.

- The risk assessment requirements provide the CPPA with a backdoor method for restricting or prohibiting risky transactions which is beyond the CPPA's authority.

- The ADMT requirements are so broadly drafted that they will inhibit business practices that have been used for decades to more accurately and efficiently service customers.

- The Proposed Regulations should be amended to more clearly exempt fraud detection practices and remove any requirements which may impede fraud detection by financial institutions.

1. The CPPA should exempt financial institutions from the definition of covered businesses for all parts of the new regulatory requirements.

SIFMA members take cybersecurity very seriously both because of longstanding regulatory requirements and because protecting client assets and information is paramount to gaining public trust and maintaining competitiveness in the industry. Moreover, compliance with regulatory mandates is not simply a matter of completing internal checklists. Financial institutions are subject to in-depth regulatory examinations on their cybersecurity, privacy, technology, and other risk management practices. If firms are found to be deficient in those reviews, then regulators can initiate enforcement proceedings. No other industry is subject to the same degree of scrutiny, and for this reason financial institutions are quite advanced in their thinking on cybersecurity, risk management, and the use of automated decisionmaking technology (“ADMT”).

However, the Proposed Regulations would impose exceedingly prescriptive requirements that may result in unnecessary compliance challenges for SIFMA members because they are also subject to, and have built robust programs adhering to, federal regulatory regimes which cover cybersecurity, risk management, and the use of automated decisionmaking technology (“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.

As such, SIFMA recommends that the CPPA 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 ADMT requirements in the Proposed Regulations. Without such an exception, financial institutions will likely be forced to divert resources away from proactively guarding against emergent threats and instead direct them toward meeting prescriptive regulatory obligations. Such diversions harm consumers rather than help them.

The legislative history of the California Consumer Privacy Act (“CCPA”) demonstrates the legislature aimed to avoid conflict with federal financial regulations by exempting data subject to federal privacy frameworks, including the GLBA. The Proposed Regulations should – indeed, they must – acknowledge and honor that policy choice. This same legislative history also demonstrates the CPPA’s authority to limit the coverage of the rules.

[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,

2. The Proposed Regulations overstep the CPPA's statutory authority.

The CPPA should amend the Proposed Regulations to align more squarely with the statutory remit for these requirements. As it stands, the Proposed Regulations go far beyond what the CCPA required or intended. For example, in Section 7123(b)(2), the draft uses an audit scheme to impose cybersecurity requirements, which are not included in the rulemaking remand. The CCPA calls on the CPPA to promulgate regulations related to cybersecurity audits, not cybersecurity requirements. We assert that the word "cybersecurity" is not mentioned in the CCPA other than the provision requiring the CPPA to promulgate cybersecurity audit regulations. The CCPA does require "reasonable security procedures and practices appropriate to the nature of personal information"; however, it does not contain "cybersecurity" requirements. The CPPA does not possess the statutory rulemaking authority to mandate cybersecurity requirements, whether explicitly or implicitly via cybersecurity audit requirements. Section 1798.100(e) of the CCPA addresses information security requirements of businesses, requiring them to implement reasonable security procedures and practices in accordance with another statute outside of the CCPA.[4]

In addition, the statutory remit for ADMT relates to the use of personal information in automated decisionmaking. The Proposed Regulations go much further than the CCPA permits as further explained below.

3. The onerous reporting obligations will outweigh any consumer benefit as the CPPA will not be able to adequately review and process this information.

The CPPA has not clearly demonstrated that the expansive Proposed Regulations are necessary to fill gaps in the cybersecurity or risk management programs of covered businesses. That is certainly not the case for federally regulated financial institutions. The burden of complying with these rules in addition to the requirements that financial institutions are already subject to will far outweigh any benefit that customers will receive. The CPPA has also not explained or attempted to explain how they will use the large quantities of data and information collected under these proposals.

The CPPA should reassess the requirements to ensure they are narrowly tailored to address important risks. Covered businesses will have to invest significant resources into complying with the Proposed Regulations that will likely be diverted from other compliance or security measures that may directly protect customers.

Also, the processing thresholds in the Proposed Regulations are extremely low and should be amended to be met if a business processes either (1) the personal information of 500,000 or more consumers or households (the Proposed Regulations stipulate 250,000 or more), or (2) the sensitive personal information of 250,000 or more consumers (the Proposed

[4] Section 1798.81.5 of the CA Civil Code, which mandates certain information security requirements of business owning or licensing personal information about state residents. Interestingly, 1798.81.5 exempts financial institutions subject to federal data security requirements. The CPPA has no rulemaking authority under CCPA Section 1798.81.5.

Regulations stipulate 50,000 or more). These increased thresholds more accurately capture significant processors of personal information and more adequately reflect the intent of the law.

At a minimum, we urge the CPPA to reevaluate the Economic and Fiscal Impact Statement and estimated costs for a typical business, which is estimated at $7,045 to $122,666 for initial costs and $26,015 in ongoing costs. SIFMA members, as noted above, are already in compliance with a robust federal regulatory regime for cybersecurity risk management which requires an audit but does not require third-party verification. We estimate that the requirement to have a yearly third-party attestation would result in $500,000 per firm in ongoing costs, on top of significant initial costs.

4. The cybersecurity audits should be aligned with existing well-established cybersecurity frameworks.

The Proposed Regulations include detailed requirements for how and what covered businesses should carry out cybersecurity audits. These regulations include prescriptive requirements for auditor independence, what the audit must cover (18 components of the cybersecurity program), and certification and timing for such audits.

These requirements conflict with federal requirements in many cases, including but not limited to the nature, independence, and characteristics of internal auditors; the requirement that the auditor report directly to the board; the requirement that the board have direct responsibility over the auditor's performance and compensation; and requiring employee training after every data breach.

The requirements should clearly align with federal regulations and national standards, particularly the National Institute of Standards and Technology ('NIST") *Framework for Improving Critical Infrastructure Cybersecurity*, but also the work that the Cyber Risk Institute ("CRI") and other organizations have done in this area. For example, most other standards are risk-based, allowing entities to be agile in adjusting to the ever-developing landscape of cyber threats. At a minimum the Proposed Regulations should be adjusted to reflect risk-based requirements rather than the prescriptive approach. In addition to aligning its requirements with these standards, the CPPA should also allow for the substitution of cybersecurity audits performed under other regimes such as NIST without having to match every requirement contemplated in the Proposed Regulations.

The CPPA should also expressly allow the use of internal auditors which meet the definition of independence and objectivity under other nationally recognized standards. The proposed standard is unclear and unnecessarily narrow. Using internal auditors will significantly save costs for SIFMA members while still retaining the necessary independence.

For financial institutions already subject to stringent federal cybersecurity audit standards, these duplicative requirements are particularly challenging as they divert financial and human resources away from more targeted and urgent risk mitigations. Having to perform a prescriptive cybersecurity audit annually will take away from a firm's ability to address the highest risk issues at a particular point in time. This is yet another reason that federally-regulated financial institutions and their affiliates should be exempted from the final regulations.

5. The risk assessment requirements provide a backdoor for the CPPA to prohibit risky transactions which are beyond its statutory authority.

The Proposed Regulations impose broad risk assessment requirements on covered businesses that process personal information which create a significant risk to the consumer's privacy or security. Such risk assessments would have to be performed before the activity commences and reviewed at least once every three years and whenever there is a material change to the processing activity. Additionally, covered businesses would be required to submit these assessments to the CPPA starting 24 months following the effective date of the final regulations.

The CPPA should more thoroughly study and consult with the business community on the breadth of the activities that would trigger a risk assessment as well as the amount of work that a covered business would have to complete to comply with the Proposed Regulations. The CPPA should further align the risk assessment requirements with others used widely by businesses, such as SOC 2 compliance reports which are already widely used and accepted in the business community. If such reports can also be used to satisfy the CPPA's requirements in their entirety, then there will be a significant reduction in burden on covered entities without increased risk to customers.

The proposed requirement to conduct and complete risk assessments within 24 months will impose an incalculable burden upon businesses. To lessen that burden, the CPPA should narrow the broad triggers for the performance of a risk assessment, narrow the unnecessarily expansive definition of ADMT, and the revise the retroactive application of this proposed risk assessment obligation such that risk assessments should only be required prospectively.[5]

The Proposed Regulations provide the CPPA with a backdoor to prohibiting processing of data which is otherwise permitted under California law but which the CPPA is not permitted to regulate. As such, the CCPA requires a business to submit a risk assessment on a regular basis to the CPPA regarding processing of personal information and whether the processing includes sensitive personal information and identifies and weighs benefits and risks (for the business, stakeholders, consumers, and the public), "with a goal of restricting or prohibiting" processing if the risk to consumers outweighs benefits to the others."[6] Section 7154 of the Proposed Regulations uses this requirement to issue regulations requiring businesses to conduct risk assessments aligned with the back door requirements to fix deficits, implement new or modified policies or procedures, and otherwise take actions not provided for within the statutory remit. This backdoor enforcement mechanism should not be permitted as risky processing is not illegal per se. Rather, risk assessments should only gauge risk versus benefit and nothing more. In sum, this section and related provisions should be deleted.

Further, the Proposed Regulations should be amended to reflect that covered businesses will not be required to divulge trade secrets as part of their risk assessments. This was mandated by the CCPA but was not expressly included in the Proposed Regulations. Further, there is no reported plan for the security of confidential information which covered businesses will be

[5] Section 7155(c).

[6] Section 1798.185(14)(B).

required by the CPPA to submit. Such a database of information is a treasure trove for cyber hackers and others seeking to take advantage of firms' vulnerabilities.

6. **The ADMT requirements may inhibit longstanding business and compliance use cases employed by financial institutions.**

The requirements for ADMT under the Proposed Regulations are very broadly drafted such that they appear to regulate a much wider range of technology than what is typically defined as ADMT under other existing standards. The definition of ADMT in Section 7001(f) should be revised to mirror other commonly accepted ADMT definitions, which are directed to wholly automated (no direct human involvement) decisionmaking processes that use personal information to make decisions with legal or similarly significant effects on consumers. Further, "legal or similarly significant effects" should be limited to effects on consumers, such as the provision of financial or lending services, housing, insurance, education enrollment or opportunities, criminal justice, employment opportunities, healthcare services, or access to basic necessities. Also, any ADMT which also includes a human in the decision-making tree should be specifically excluded from the application of the Proposed Regulations.

The inclusion of behavioral advertising within the definition of ADMT in the Proposed Regulations will present a significant challenge for SIFMA members. This broad definition encompasses practices used by firms for decades to efficiently connect customers with products and services that make sense for them. The definition should be modified to specifically exclude profiling for the purpose of better understanding customers and managing internal risk controls, as well as customer service. In addition, SIFMA members are already subject to extensive requirements under existing SEC and FINRA advertising and marketing rules. Such regulated activities should be outside the scope of this rulemaking.

Furthermore, a wide range of SIFMA members' long standing business activities in the areas of fraud detection, cybersecurity, trading algorithms, portfolio analysis, trade routing, and other basic uses may be impacted by this rule if finalized as proposed. The Proposed Regulations could be read to include the use of Excel spreadsheets which was likely not intended. For financial institutions, these basic uses of ADMT provide for efficiency, enhanced supervision, and leveraged use of technology to ensure the financial markets are well-run. Financial institutions' use of such ADMTs are also extensively regulated, examined, and enforced by federal financial regulators. The Proposed Regulations have the potential to inflict unnecessary upheaval in the day-to-day operations of the financial services industry without any obvious benefits.

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

In their current form, the Proposed Regulations potentially constrain fraud prevention activities as well as other legal and compliance activities conducted by financial institutions. The Proposed Regulations would specifically exempt from consumer ADMT opt-out requests:

> *The business's use of that automated decisionmaking technology is necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below ("security, fraud prevention, and safety exception"):*
>
> *(A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;*
>
> *(B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or*
>
> *(C) To ensure the physical safety of natural persons.*[7]

This proposed exemption does not go far enough, however. For example, this does not sufficiently allow firms to defend against illegal actions, such as money-laundering, which are not directed at the financial institution per se, but instead at the federal government or the financial system writ large. With instances of fraud increasing rapidly, along with the sophistication of schemes, it's crucial that the financial services industry use every tool available, including advancements in technology, to continuously refine and bolster fraud detection and supervision programs. 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. Such uses are clearly not the intended targets of the law or the Proposed Regulations but are widely used in the financial services industry.

In addition, the exemption seems to grant fraudsters access rights to a financial institution's data which may show them how the financial institution's algorithm detects fraud and give them the opportunity to learn how to avoid their detection in the future.

- Finally, there should be no opt-out or other restrictions that may impede a financial institution's ability to detect and report suspicious activity, suspected money laundering, Foreign Corrupt Practices Act ("FCPA") violations, fix account errors, notify customers of suspicious account activity, or other compliance related functions. Such use cases benefit customers, and the financial system as a whole and therefore should be specifically permitted under the rules. Additionally, if an individual decides to opt-out, it can have significant impact on

[7] Section 7221(b)(1).

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.

* * * * *

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