sifma

Invested in America

March 27, 2023

VIA E-Mail to regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR 02-2023 - INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING

Dear California Privacy Protection Agency,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to provide feedback on the California Privacy Protection Agency ("CPPA") Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking dated February 10, 2023.[2] SIFMA members take cybersecurity and data protection seriously as it is a key component of client trust and confidence. In addition, SIFMA members are subject to a wide array of federal, state, and international laws and regulations governing cybersecurity and data protection. There are also significant requirements in place that would govern SIFMA members' use of artificial intelligence ("AI") that should also be considered in any CPPA rulemaking or guidance.

---

1 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 nearly 1 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 California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking* (February 10, 2023) (available at https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf).

A. The CPPA rules governing cybersecurity risk and AI should take into account existing laws and regulations.

Most critically, the CPPA should take into consideration existing and future federal and state requirements and ensure that any rules promulgated closely align and provide sufficient flexibility to achieve compliance without unnecessary additional burdens on covered entities. To that end, any assessments or audits that companies perform as subjects of federal or state cybersecurity and artificial intelligence laws, regulations, or frameworks should also satisfy any related CPPA audit and assessment requirements.

Specifically, SIFMA members or their affiliates are already subject to, or will be subject to the following cybersecurity requirements:

- The SEC has proposed cybersecurity risk management rules that would require broker-dealers, investment advisers, funds, and other entities to periodically assess and draft documentation of cybersecurity risks.[3] The proposed rules also provide factors that must be considered when conducting risk assessments. Additionally, existing rules and recent SEC enforcement actions indicate that firms should take a risk-based approach in effectively managing cyber risks, which is the approach already taken by many financial institutions.

- FINRA explains in its Cybersecurity Report that broker-dealer firms should conduct a cybersecurity risk assessment or risk-based audit to determine risks in developing cybersecurity programs.[4]

- GDPR requires companies that engage consumers in the United Kingdom or European Union to conduct a Data Protection Impact Assessment where the processing data is likely to result in a high risk of harm to the rights and freedoms of natural persons who reside in those jurisdictions.[5]

---

[3] *See* Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34-97142 (March 15, 2023); Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release No. 34-94197 (Feb. 9, 2022).

[4] *See* FINRA Rules Related to Cybersecurity, available at https://www.finra.org/rules-guidance/key-topics/cybersecurity#rules.

[5] *See* Article 35, EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679.

- The New York Department of Financial Services ("NYDFS") Cybersecurity Regulation requires a periodic cybersecurity risk assessment. [6]

Similarly, when considering rules governing AI, the CPPA should consider the extensive risk management frameworks that financial institutions already have in place, including frameworks that address oversight and assessment of AI and automated decisionmaking more broadly within financial institutions, of which privacy considerations are one aspect when personal information is involved. In particular, the CPPA should consider whether such requirements would already be addressed or are currently being considered by financial services regulators.

The CPPA should take the following into consideration when proposing additional regulations pertaining to AI:

- California's Department of Insurance released Bulletin 2022-5 which discussed obligations on insurance company obligations to ensure there is not unfair discrimination as a result of the use of artificial intelligence/Big Data analytics.[7]

- NIST AI Risk Management Framework is intended to help build trustworthiness in AI design and development.[8]

- FINRA published a report on AI in the financial services industry finding that firms were taking a cautious but useful approach to using AI in various aspects of the business but did not cite any significant regulatory concerns.[9]

- The Office of the Comptroller of the Currency ("OCC") released supervisory expectations for using AI last year.[10]

---

[6] *See* 23 NYCRR 500.9.

[7] *See* Bulletin 2022-5, California Department of Insurance (June 30, 2022), available at https://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/BULLETIN-2022-5-Allegations-of-Racial-Bias-and-Unfair-Discrimination-in-Marketing-Rating-Underwriting-and-Claims-Practices-by-the-Insurance-Industry.pdf.

[8] *See* NIST AI Risk Management Framework (January 2023), available at https://www.nist.gov/itl/ai-risk-management-framework.

[9] *See* FINRA Report, Use of Artificial Intelligence (AI) in the Securities Industry (June 10, 2020), available at https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry ("FINRA AI Report").

[10] *See* OCC News Release 2022-52, Deputy Comptroller Testifies on Artificial Intelligence (May 13, 2022), available at https://occ.gov/news-issuances/news-releases/2022/nr-occ-2022-52.html.

B. Cybersecurity audits and risk assessments should be risk-based, independent, non-public, and track existing requirements adopted in other jurisdictions.

The California Privacy Rights Act ("CPRA") requires covered entities to conduct both annual cybersecurity audits and "regular" risk assessments. Audits must be performed by the covered entity, but the entity must establish the scope of the audit and also ensure the audit is independent. Risk assessments must be submitted to the CPPA and must disclose whether the covered entity's processing includes sensitive personal information. If the processing does include sensitive personal information, the business must identify any risks and benefits of processing such information with a goal of minimizing such processing if the risks outweigh the benefits to the consumer.

SIFMA appreciates the importance of periodic cybersecurity audits and risk assessments as they are an efficient way for companies to review their policies and find areas of weakness and risk without exposing the firm to additional risk. As demonstrated by the list of existing requirements above, financial institutions already undergo significant risk assessments and audits for various purposes. As such, any implementing regulations should reenforce that both the audit and the risk assessment are risk-based requirements. Further, covered entities should be expressly permitted to use third-party assessments, such as SOC 2 Type 2, to meet the CPRA criteria.

Annual audits should be risk-based to take into account the business activities, size, and other factors that may impact cyber risk. As such, covered entities should not be required to review every aspect of their cybersecurity programs every year if there is not a sufficient risk-based reason to perform such a review. In addition, firms could use resources to take deeper dives on certain issues as necessary without wasting resources on reviewing issues that are low risk. Any cybersecurity audit should be "independent," but such a requirement should also expressly permit internal auditors or an affiliate to perform the audit if they meet the independence standard. Most large companies have robust internal audit capabilities which can achieve the same results as any external auditor.

Further, audits and risk assessments should not be required to be made public. Public disclosure of such audits or risk assessments puts companies and the cyber ecosystem as a whole at significant risk as such documents can provide a roadmap for bad actors.

C. Regulation of automated decisionmaking and artificial intelligence should be principles-based and consider the extensive risk management processes that financial institutions already have in place.

The growing use and capabilities of automated decisionmaking and artificial intelligence (together, "AI") have understandably captured the attention of the public and regulators in a broad range of sectors. It makes sense for financial services regulators to increase their understanding and the public's understanding of how AI is used, evidence

related to perceived risks, and how actual risks are being addressed. Close and ongoing discussions and exchanges of information between regulators and industry are especially important. For all these reasons, the CPPA's request for feedback is an important step in a valuable process.

The financial services sector does, however, have unique and important differences, when compared to other major industries, in its treatment of AI-related risks and capabilities. Established financial institutions already have sophisticated systems in place for overseeing a broad variety of risks, including risks posed by using AI in various contexts. Financial service providers have devised and implemented these risk management frameworks with extensive input from federal financial services regulators, at both the policy and implementation levels.

Senior managers and boards of financial institutions devote considerable resources to ensuring the adequacy, flexibility, and adaptability of those systems and processes to identify, quantify, and mitigate risks of various types. The resulting risk management systems typically involve both focused accountability and cross-function and cross-divisional processes. Firms measure the resulting effectiveness of these processes with a range of established and evolving tools. As different types of asset, personnel, macroeconomic, and process risks emerge and are addressed, institutions test, refine, and expand the capabilities of their risk management processes.

At the same time, financial institutions' uses of AI capabilities are not new, and their consideration and management of risks related to those uses are well developed. Financial institutions have used automated methods of processing customer information, monitoring and protecting against fraud, assessing financial performance and risk, evaluating credit risk, assessing value at risk, and discharging many other functions.[11] In recent years, the "artificial" capabilities associated with these processes have grown more sophisticated. Likewise, financial institutions have undertaken an equally long and continuous process of identifying, monitoring, and mitigating risks associated with using those capabilities.

Further, as we recommended above for cybersecurity audits and risk assessment, the CPPA should consider any assessments of AI used to satisfy other federal or state requirements should also satisfy regulations promulgated under CPRA.

* * *

[11] *See* FINRA AI Report.

SIFMA appreciates the opportunity to provide feedback on the CPPA's proposals and would be pleased to discuss these comments in greater detail. If you have any questions or would like to schedule a meeting, please contact me at mmacgregor@sifma.org.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director, Deputy General Counsel & Corporate Secretary