BizFed Los Angeles County Business Federation
Strengthening the Voice of Business Since 2008

SVLG
SILICON VALLEY LEADERSHIP GROUP

California Black Chamber of Commerce
"Dedicated to Economic Empowerment"

CALASIAN chamber of commerce

NFIB

BizFed Central Valley Business Federation
Strengthening the Voice of Business

CALIFORNIA HISPANIC CHAMBERS OF COMMERCE
EST. 1978

LOS ANGELES AREA
CHAMBER OF COMMERCE

CALIFORNIA RESTAURANT ASSOCIATION

CALIFORNIA ATTRACTIONS AND PARKS ASSOCIATION
CAPA

CMTA
CALIFORNIA MANUFACTURERS & TECHNOLOGY ASSOCIATION

CHAMBER OF PROGRESS

CALIFORNIA AFRICAN AMERICAN
CHAMBER OF COMMERCE

TechCA

CHAMBER
SAN MATEO COUNTY

MAKING YOUR BUSINESS OUR BUSINESS
LBA
LATIN BUSINESS ASSOCIATION®
ESTABLISHED 1976

SAN JUAN CAPISTRANO
EST. 1923
CHAMBER OF COMMERCE

ECONOMY BUSINESS POLICY
SAMCEDA
San Mateo County Economic Development Association

COALITION of CALIFORNIA CHAMBERS
ORANGE COUNTY

BAYAREA COUNCIL

SANTA BARBARA
SOUTH COAST
CHAMBER OF COMMERCE
FROM GOLETA TO CARPINTERIA

VALLEY INDUSTRY & COMMERCE ASSOCIATION
VICA 75th
ANNIVERSARY YEAR
1949 2024

FLASHER BARRICADE ASSN.

CF CA
CALIFORNIA FUELS + CONVENIENCE ALLIANCE

ALLIED MANAGED CARE INCORPORATED

AIMS℠
ACCLAMATION INSURANCE MANAGEMENT SERVICES

Sd
San Diego Regional Chamber

ORANGE COUNTY BUSINESS COUNCIL

United Chambers of Commerce
Of the San Fernando Valley

CalABC
California Automotive Business Coalition
Representing Industry to Government since 1992

M
MULTICULTURAL BUSINESS ALLIANCE

DTLA CHAMBER

ecomback

FAMILY BUSINESS ASSOCIATION
OF CALIFORNIA

ASIAN INDUSTRY B2B
IMPACTING THE SOCAL COMMUNITY

B

CHATSWORTH PORTER RANCH
EST. 1914
CHAMBER of COMMERCE

Coalition of Small & Disabled Veteran Businesses

GACOC
Greater Arden Chamber of Commerce
Where business happens

San Jose Chamber of Commerce

AHLA
AMERICAN HOTEL & LODGING ASSOCIATION

January 13, 2025

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Dear California Privacy Protection Agency Board Members and Staff,

The undersigned business associations and chambers of commerce remain in opposition to the California Privacy Protection Agency's ("Agency" or "CPPA") moving forward with the proposed regulations regarding Automated Decision-making Technology ("ADMT"), risk assessments, and cybersecurity. The proposed regulations will impose unnecessary burdens and costs on CA businesses that don't advance consumer privacy and exceed the mandate given to the CPPA. We strongly urge the CPPA to withdraw the proposed regulations and work with Governor Newsom and the Legislature to develop more effective and less costly ADMT, risk assessment, and cybersecurity policies.

The CPPA's proposed regulations will significantly increase costs for business owners and consumers and will reduce state revenues that fund high priority programs. The Standardized Regulatory Impact Assessment (SRIA) prepared in conjunction with the proposed regulations reveals that more than 52,000 California businesses will be required to comply with regulations that will have a $3.5 billion impact on the economy. Business costs will also grow amid our current inflation as small operations will need to hire legal and compliance staff to help unpack the new rules, further impacting consumer concerns about the cost of living.

The SRIA concludes that the regulation will result in employment losses in early years, peaking at 126,000 in 2030 and annual state revenue losses peaking at $2.8 billion in 2028. The SRIA also speculates that those costs will be offset in the future by savings but the business community has heard that prediction many times and the savings rarely materialize. At a time when the state "faces double-digit operating deficits in the years to come" according to the LAO's CA Fiscal Outlook, these additional revenue losses will devastate California.

The proposed regulations are beyond the scope of the CCPA and AI rules should be developed by the Legislature and the Newsom Administration where the full range of costs and benefits, including budget impact, can be fully debated and decided by democratic process. At the November 8 Agency meeting, Board member and author the California Privacy Rights Act Alastair Mactaggart rightly voiced concerns that the scope of the proposed rules exceeds the intent of the California Consumer Privacy Act, and diverse speakers from the state's business community echoed fears that the rules would result in significant costs to state businesses, tens of thousands of jobs lost and reduced capital for investment and innovation.

Instead of proceeding with the proposed regulations, the CPPA should work with Governor Newsom and the Legislature to provide input on how to reduce the unnecessary burdens on business and adopt a risk-based approach that focuses on business activities that pose meaningful risks to consumers.

The proposed regulations will stifle innovation and advancements that are already providing benefits to consumers and business. They will impose significant burdens to California consumers, innovators and businesses. For example, the proposed rules around ADMT pop-ups will create significant burdens for those wishing to conduct research or transact business over the internet. In addition to separate notifications regarding consent for cookies and promotional communications, users will now face further pop-ups, one for receiving information on ADMT, and a second regarding the use of ADMT for delivering advertising based on prior activity. California consumers should not be impeded at each step of an online transaction. The value of individualized privacy notices of specific practices diminishes each time a new specialized notice is required and the list of such notices gets longer – it is unrealistic to think that consumers will carefully review multiple pop-ups preventing them from accomplishing their purposes for being online. The Agency needs to review the notice requirements in the proposed regulations and eliminate individualized notices for anything other than true high risk activities that expose consumers to privacy harms. Consumers benefit most from a notice regime that *successfully* draws their attention to important information about privacy practices. Simplifying notice requirements benefits consumer privacy and reduces costs to businesses. Likewise, cybersecurity audit and risk assessment regulations are far more burdensome than necessary to achieve their goals. There are many expert-developed and internationally recognized risk management frameworks and standards that are better suited to guiding these processes and provide the additional benefit of harmonizing compliance requirements across jurisdictions, lowering business costs while protecting consumers.

The proposed regulations will unduly interfere with consumer use of the internet and result in frustrated consumers leaving a site before completing a transaction, or leaving before the business could share important information with users. This unintended consequence is especially pronounced for small and local businesses who depend on online commerce to supplement their limited physical presence and businesses that exist solely online. Restrictions on the use of ADMT and AI could harm small businesses by limiting their ability to use digital tools to reach consumers, share offerings and conduct transactions. Because the proposed regulations impose substantial burdens on low risk uses of ADMT rather than focusing on consequential decisions with legal or similar impact on consumers, such as by treating advertising as though it is on par with hiring and mortgage loan decisions, businesses are discouraged from using AI in ways that can bring increased efficiency, productivity, growth and expansion. The AI opportunities lost are not captured by the SRIA.

The CPPA should withdraw the proposed regulations and coordinate their regulatory efforts with Governor Newsom and the Legislature. While we understand and agree that having consumer protection guardrails is important as technology evolves, it is essential that such rules be the product of a robust and deliberative process. We are concerned that the Agency is developing a framework for regulating AI without providing sufficient opportunity to receive or consider feedback from all stakeholders. A process of this scope should be led by the Legislature, where the matters under consideration can be publicly-debated and determined first by elected officials. Additionally, the Agency finds itself out-of-step with the Governor's Executive Order on AI that directs state agencies to consider how to deploy AI for the benefit of Californians, while avoiding an incongruous patchwork of agencies issuing their own discordant technology rules. Despite Agency efforts at stakeholder engagement, there has been no meaningful debate among stakeholders and the Agency has not taken on board any of the feedback provided.

California is the global leader in AI research, development and deployment. The industry undergirds our Innovation Economy and the small businesses that benefit from the online tools and services it provides. Rushing to regulation harms California consumers, small businesses and our state economy. The high upfront costs of the proposed regulations will siphon resources away from innovation, depriving Californians from the benefits of new and refined commercialized technologies and greatly exacerbating the state's budget deficit. Considering the range of state-funded programs, services, and benefits that will need to be cut as a result of the rules, the voters should be represented in making these decisions. In sum, California workers, residents and businesses cannot afford the proposed rules.

Thank you for the opportunity to comment on the proposed regulations.

Sincerely,

Silicon Valley Leadership Group
Los Angeles County Business Federation
California African American Chamber of Commerce
California Asian Chamber of Commerce
California Black Chamber of Commerce
California Hispanic Chambers of Commerce
National Federation of Independent Business
California Restaurant Association
EcomBack
California Attractions and Parks Association
Acclamation Insurance Management Services (AIMS)
Allied Managed Care (AMC)
Flasher Barricade Association (FBA)
Coalition of Small and Disabled Veteran Businesses
MultiCultural Business Alliance
San Mateo County Economic Development Association
Los Angeles Area Chamber of Commerce
Bay Area Council
Santa Barbara South Coast Chamber of Commerce
San Juan Capistrano Chamber of Commerce
Coalition of California Chamber - Orange County
Chamber San Mateo County
Orange County Business Council
San Diego Regional Chamber of Commerce

TechCA
Family Business Association of California
Chamber of Progress
United Chambers of Commerce of the San Fernando Valley
California Automotive Business Coalition
California Fuels & Convenience Alliance
Latin Business Association
Valley Industry & Commerce Association
DTLA Chamber of Commerce
Asian Industry B2B
Greater Arden Chamber of Commerce
San José Chamber of Commerce
Chatsworth Porter Ranch Chamber of Commerce
Beach Real Estate Group
American Hotel & Lodging Association

From: Joshua Smith <Joshua.Smith@bpi.com>
Sent: Tuesday, January 14, 2025 9:16 AM
To: Regulations@CPPA
Subject: Bank Policy Institute: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Bank Policy Institute comment letter (Jan. 14, 2025).pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear California Privacy Protection Agency,

Please find attached a comment letter from the Bank Policy Institute.

We appreciate the opportunity to comment and thank you for your review.

Best,

Josh Smith
Vice President, Assistant General Counsel
Bank Policy Institute
joshua.smith@bpi.com | (202) 589-2534

BANK POLICY INSTITUTE

January 14, 2025

Via electronic mail

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

Re: **Comments on Proposed Cyber, Risk, and ADMT Rules**

The Bank Policy Institute[1] appreciates the opportunity to submit comments to the California Privacy Protection Agency ("Agency") on its rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking technology ("ADMT") under the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA").[2]

I. Executive Summary

BPI's members have invested significant time and resources into building data protection and information security systems and automated decisionmaking models that align with state and federal financial privacy, consumer protection, and other financial services laws and regulation. BPI members are committed to promoting robust privacy protections for California consumers. As described in greater detail below, banking organizations[3] are heavily regulated and subject to close supervision on cybersecurity, risk, and automated decisionmaking matters. Among other areas of extensive regulation and supervision, banking organizations are required to maintain robust internal security controls to protect their information systems, maintain effective risk assessment and model risk management processes, and comply with various transparency obligations with respect to automated tools.

The proposed rulemaking exceeds the limits on the Agency's authority, including because the Agency does not have authority under the CCPA framework to develop a cybersecurity control framework or to regulate certain processing activities covered by the proposed new rules. For example, to

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. BPI produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues.

[2] Cal. Civ. Code § 1798.100 *et seq*.

[3] Throughout, BPI uses the term "banking organization" to refer to national and state banks and savings associations and their affiliates, as well as foreign banking organizations and their U.S. branches to the extent the California rules purport to apply to them.

avoid exceeding its statutory authority, the Agency must focus its automated decisionmaking regulations on *significant decisions concerning a consumer.*

Most of the personal information processed by banking organizations is subject to the Gramm-Leach-Bliley Act ("GLBA") and therefore exempt, by statute, from the CCPA and its implementing regulations. However, the proposed regulations would impose obligations on all businesses, even banking organizations that process only limited information subject to the CCPA. In doing so, the proposed rules would impose backdoor requirements on data subject to GLBA via rules that can only be satisfied through enterprise-wide compliance processes and negatively affect critical bank operations and services that may involve processing various types of personal data, such as safe and sound underwriting for certain small businesses, fraud prevention, and information security activities.

As a result, all three sets of proposed rules have applications that would interfere with banking activities performed by banking organizations and therefore would be subject to federal preemption. Moreover, elements of the proposed regulations would, if applied to banking organizations, interfere with the exclusive visitorial powers granted to federal regulators, irrespective of the application of the GLBA. California cannot *directly* audit these banking activities, and so it cannot *indirectly* achieve that result by having banks conduct a highly prescriptive audit on its behalf. These obligations result in the Agency effectively inspecting and supervising banking activities, which is the exclusive purview of prudential regulators under long-established legal principles.

Even if not preempted, the application of new state regulations to banking organizations could undermine and conflict with existing legal regimes applicable to banking organizations. For example, the regulations introduce prescriptive cybersecurity audit requirements that seemingly require a single annual information security audit. This requirement is in tension with the more rigorous approach to cybersecurity audits of banking organizations, which often conduct detailed, area-specific audits and approach cybersecurity audits on a rolling basis rather than an annual basis. As another example, the draft automated decisionmaking regulations are in tension with how banking organizations manage their lending and credit risk management activities to facilitate and protect the U.S. banking system. If bad actors must be given information about or may opt out of the use of their data for training automated fraud detection, there is risk to the safety and soundness of the banking system, which could ultimately limit banking organizations' ability to extend certain small business loans and other financial products and services.

BPI urges the Agency to exempt from the three new proposed rules financial institutions that are subject to examination or supervision by a federal prudential regulator and their affiliates.[4] This exemption would avoid conflict with visitorial rights and preemption principles and sensibly avoid conflict with these organizations' already robust federal regulation and supervision. The Agency unquestionably has authority to create such an exemption; indeed, its rulemaking authority contemplates that its regulations should "further the purposes of" the CCPA, which include designing cyber audit and risk assessment protections for businesses whose processing of personal information presents *significant risk* to consumer privacy and security. It does not serve these purposes to impose the proposed requirements on banking organizations and their affiliates that are subject to prudential examination or supervision on these same issues and process limited personal information that is subject to the CCPA framework.

If the Agency does not include an exemption for banking organizations, it must make additional changes to avoid imposing requirements on banking organizations that would result in unintended and

[4] The Agency should keep in mind that affiliates of a bank in a banking holding company structure are subject to consolidated supervision by the Federal Reserve.

detrimental impacts to the banking system, including by implementing the specific recommendations described below. To echo Board member Alastair Mactaggart, the current regulations "undermine[] privacy" in favor of "overreach, [a] lack of privacy protection, and [a] high likelihood of legal challenges." The Agency must revise its regulations in order to avoid these consequences. In an appendix, we suggest in-line changes implementing the suggestions within this letter.

II. Banking Organizations are Already Subject to Comprehensive Cybersecurity Audit, Risk Assessment, and ADMT Requirements.

Federal financial regulators already closely supervise the cybersecurity and risk assessment practices and use of automated decisionmaking by banking organizations and their affiliates.[5] Banking organizations are required to have effective risk management controls for these activities, which are reviewed both by banks' independent audit function and by federal prudential regulators that conduct examinations of banks (including on-site examinations). Of note, these requirements stem not only from the GLBA, but also from other federal banking legal and regulatory requirements and supervisory practices. Banking organizations are subject to "safety and soundness" supervision under standards that require banks to engage in risk assessments, maintain robust internal security controls to protect their information systems and model risk management processes, and provide transparency to consumers in relation to use of certain models.[6] More specifically:

- *Cybersecurity Audits.* Banking organizations are subject to extensive regulation and supervision under safety and soundness standards that address whether banking organizations assess, implement, and audit effective internal controls for their information systems.[7] These entities' information security programs must be tested and evaluated through internal audits, self-assessments, tests, and exercises in accordance with extensive guidance promulgated by federal prudential regulators on these audits.[8] In addition, under GLBA, a financial institution is similarly required to regularly monitor, evaluate, and adjust its information security program, including assessing whether certain enumerated controls are appropriate to deploy (e.g., access controls and

[5] These regulators include federal prudential regulators (i.e., Board of Governors of the Federal Reserve System ("Board"), Federal Deposit Insurance Corporation ("FDIC"), and Office of the Comptroller of the Currency ("OCC")) and, for state-chartered financial institutions, state banking regulators in addition to federal prudential regulators. The federal prudential regulators have developed an extensive inventory of policy statements, toolkits, and other guidance that set regulatory expectations for banks' information security, model risk management, and audit programs, including "regarding the security of all information systems and information maintained by or on behalf of a financial institution" across GLBA and non-GLBA data. FFIEC, IT EXAMINATION HANDBOOK: INFORMATION SECURITY at 1 n.4 (Sept. 2016), *available at* https://ithandbook.ffiec.gov/it-booklets/information-security/ ("Information Security Booklet"); *see also* OCC, COMPTROLLER'S HANDBOOK: MODEL RISK MANAGEMENT (Aug. 2021), *available at* https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html ("Model Risk Management Booklet").

[6] 12 U.S.C. §§ 1818, 1831p-1; 12 C.F.R. § 30, Appendix A (OCC) ("Interagency Guidelines Establishing Standards for Safety and Soundness"); 12 C.F.R. § 208, Appendix D-1 (Board); and 12 C.F.R. § 364, Appendix A (FDIC).

[7] Interagency Guidelines Establishing Standards for Safety and Soundness at Sections II.A and II.B.

[8] *Id.*; *see also* Information Security Booklet at 53; OCC, COMPTROLLER'S HANDBOOK: INTERNAL AND EXTERNAL AUDITS at 2, 112 (July 2019), *available at* https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/internal-external-audits/pub-ch-audits.pdf ("Comptroller's Handbook"); FFIEC, IT EXAMINATION HANDBOOK: AUDIT at A-1–A-17 (April 2012), *available at* https://ithandbook.ffiec.gov/it-booklets/audit/ ("Audit Booklet"); OCC Bulletin 2003-12: Interagency Policy Statement on Internet Audit and Internal Audit Outsourcing; and OCC Bulletin 99-37: Interagency Policy Statement on External Auditing Programs.

encryption).[9] These requirements extend to both GLBA and non-GLBA data. The prudential regulators require that "all elements of the information security program must be coordinated" across "all parts" of a banking organization.[10]

Banking regulators have designed these requirements to be compatible with existing frameworks and best practices, recognizing "the benefits of using a standardized approach to assess and improve cybersecurity preparedness."[11] Thus, banks use widely accepted cybersecurity control frameworks as the basis for their cybersecurity audits, such as the NIST Cybersecurity Framework ("NIST CSF") or the CRI Profile (which was designed in collaboration with prudential regulators based on NIST CSF and incorporates existing financial regulatory requirements and globally recognized standards).[12]

Financial institutions also need to navigate a broader cyber regulatory environment, including requirements set by their home state chartering authorities for state-chartered institutions. State financial regulators in some jurisdictions have set out robust requirements that state-chartered banks and other state licensees maintain a cybersecurity program that is based on a risk assessment, tested, and audited. Among such state requirements, the New York Department of Financial Services has requirements that mandate annual certifications of compliance for state chartered banks and licensees. As another example, broker dealers and others within the jurisdiction of the Securities and Exchange Commission ("SEC") are subject to a separate set of information security rules.[13]

- *Risk Assessments.* As part of ensuring a banking organization operates in a safe and sound manner, federal regulations and guidance already require risk assessments across the organization's business activities.[14] These include risk assessments in relation to processing activities involving personal information, although the triggers for these assessments are not solely focused on activities that involve personal information. As one example, when banking organizations seek to define security controls for new, revised, or newly required applications, they are required to begin with a risk assessment under which they consider the risks to the data and the system (e.g., the potential impact of unauthorized access or damage), along with the characteristics of the information at risk.[15]

[9] 12 C.F.R. § 30, Appendix B at Sections II and III ("Interagency Guidelines Establishing Information Security Standards").

[10] *Id.* at Section II.A.

[11] Press Release, FFIEC, FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness (Aug. 28, 2019), *available at* https://www.ffiec.gov/press/pr082819.htm.

[12] *See* Comptroller's Handbook at 112; *see also* NAT'L INST. OF STANDARDS AND TECH, THE NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf ("NIST Cybersecurity Framework"); CYBER RISK INST., THE PROFILE, *available at* https://cyberriskinstitute.org/the-profile/ ("CRI Profile").

[13] 17 C.F.R. § 248.30 (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information); *see also* 16 C.F.R. § 314 (Safeguards Rule); Regulation (EU) 2022/2554 (EU Digital Operational Resilience Act).

[14] Interagency Guidelines Establishing Standards for Safety and Soundness at Section II.A; *see also* 12 C.F.R. § 30, Appendix D (outlining requirements for large OCC-regulated banks).

[15] Information Security Booklet at 39; *see also id.* at 25 and 34.

There are also separate regimes, such as the Fair Credit Reporting Act, that require risk assessments in certain scenarios (e.g., identity theft prevention).[16] Moreover, the GLBA further requires these entities to identify threats to the security, confidentiality, and integrity of customer information and then assess the sufficiency of their policies, procedures and other measures to control risks that could potentially result from these threats.[17] As a matter of practice, banking organizations will take these requirements into account across all of their data and systems.

- *Automated Decisionmaking.* Federal regulators review banking organizations' adoption of new technology and closely monitor the use of artificial intelligence in order to ensure that financial institutions operate in a "safe and sound manner" and in compliance with applicable laws and regulations. Banking organizations are uniquely subject to model risk management guidance governing their use of models, which include artificial intelligence models. [18] This guidance addresses concerns such as uncertainty about inputs and assumptions, inaccurate outputs, discriminatory power, precision, accuracy, robustness, stability, reliability, and other misapplication or misuse of models.[19] Among other requirements, federal guidance contemplates that AI models should be subject to appropriate and effective due diligence, inventorying, risk assessments, technology controls, and processes to validate that the model provides sound, fair, and unbiased results.

  Banking organizations are also uniquely subject to federal supervision of their models, with regulators often establishing an ongoing presence within the banks themselves to monitor compliance. Among other topics, federal supervision addresses model validation, development, testing, and use; governance, including board oversight and personnel requirements; and relevant third-party relationships.[20] Indeed, the banking regulators subject banking organizations' use of emerging technology to excessive supervision, not too little.[21]

  Federal regulators continue to emphasize that existing laws create a robust regulatory framework applicable to the use of automated decision-making tools. For example, Federal Reserve Vice Chair for Supervision Michael Barr has advocated for using existing frameworks to allow banks to "continue to innovate" while "guard[ing] against . . . downside risks."[22] Additionally, Federal

[16] *See, e.g.,* 12 C.F.R. § 41, Subpart J (Red Flags Rule) (requiring theft prevention programs, which involve the identification of red flags for identity theft and protocols to address identity theft).

[17] Interagency Guidelines Establishing Information Security Standards at Section III.

[18] Model Risk Management Booklet at 13. Note that, while AI technology may not always fit within the definition of a "model" for purposes of Board SR Letter 11-7, OCC SR 11-12, or FDIC FIL-22-2017, the flexible and risk-based principles of the model risk management framework provide principles and processes that banking regulators expect banking organizations' to regularly apply to address new types of models and technology that were not originally contemplated when the guidance was issued. See discussion below.

[19] OCC Bulletin 11-12: Supervisory Guidance on Model Risk Management; Board SR Letter 11-7: Guidance on Model Risk Management; and OCC Bulletin 11-12 at 3–4.

[20] *See generally id.*

[21] *See, e.g.,* Paige Pidano Paridon & Joshua Smith, Distributed Ledger Technology: A Case Study of The Regulatory Approach to Banks' Use of New Technology, BANK POL'Y INST. (Feb. 1, 2024), *available at* https://bpi.com/distributed-ledger-technology-a-case-study-of-the-regulatory-approach-to-banks-use-of-new-technology.

[22] Federal Reserve Boston, Minneapolis Fed President Neel Kashkari Fireside Chat with Vice Chair for Supervision Michael S. Barr, YOUTUBE, at 24:30, *available at* https://www.youtube.com/watch?v=qYLNmtPgtGo&t=4s ("Remarks by Vice Chair Barr").

Reserve Governor Michelle Bowman has explained that banking organizations' use of AI must comply with relevant laws governing fair lending, cybersecurity, data privacy, third-party risk management, and copyright, adding that "when AI is deployed in a bank, an even broader set of requirements may apply depending on the use case."[23]

Indeed, banks are subject to several industry-specific laws, regulations, and guidance intended to achieve accountability, accuracy, and transparency in bank decisionmaking. Among them, the Equal Credit Opportunity Act ("ECOA") and Regulation B (which implements ECOA) prohibit unlawful discrimination against protected classes in "any aspect of" credit transactions, including through the use of automation for credit underwriting and credit servicing.[24] ECOA and Regulation B also provide certain notice requirements and data access rights. These include a right to a statement of reasons for a creditor taking adverse action, including reasons based on automated decisionmaking tools, and a copy of any written appraisals and valuations for certain mortgage loan applications.[25] The Fair Credit Reporting Act ("FCRA") similarly creates notice obligations regarding adverse decisions and rights to access and dispute information in consumer reports that may be used to facilitate decisions relating to credit, insurance, or employment.[26] Moreover, automated decisionmaking technologies that produce outcomes with legal or similarly significant effects on an individual (e.g., the denial or provision of financial services) may be subject to these ECOA and FCRA provisions. These and other regimes also protect against discrimination through automated decisionmaking. For example, the federal Fair Housing Act prohibits discrimination in the sale or rental of housing, residential real estate transactions, or the provision of real estate brokerage services, including through automated decisionmaking.[27]

To the extent additional regulation becomes needed, federal regulators have made clear they are prepared to update the regulatory framework. For example, as banks moved towards increased reliance on automated credit underwriting, the prudential regulators issued a policy statement

[23] Michelle W. Bowman, Gov., Fed. Reserve, Address at 27th Annual Symposium on Building the Financial System of the 21st Century: An Agenda for Japan and the United States: Artificial Intelligence in the Financial System (Nov. 22, 2024), *available at* https://www.federalreserve.gov/newsevents/speech/bowman20241122a.htm ("Speech by Gov. Michele Bowman"). Governor Bowman also called for a "gap analysis to determine if there are regulatory gaps" and for enhanced "coordination both within each agency and among domestic regulators that play a role in the supervision and regulation of the financial system." *Id.* This underscores federal banking regulators' attentiveness to challenges posed by emerging technologies in the banking industry, as well as their commitment to the ongoing development of sector-specific regulation.

[24] 15 U.S.C. § 1691 *et seq.*

[25] 15 U.S.C. § 1691(d), (e); 12 C.F.R. §§ 1002.9(b)(2),1002.14; *see also* CFPB, Consumer Financial Protection Circular 2022-03 (addressing adverse action notice requirements in connection with credit decisions based on complex algorithms); CFPB, Consumer Financial Protection Circular 2023-03 (addressing the requirement to provide reasons in adverse action notices even when making decisions based on complex algorithms). Indeed, Circular 2023-03 likely *over*states, not understates, what is required by law in these circumstances. *See generally*, Letter from Kathleen C. Ryan, Senior Vice President, Am. Bankers Ass'n, to CFPB, FDIC, FRB, and OCC (Feb. 12, 2024), *available at* https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2024/02/02122024-letter-to-agencies-effective-agency-guidance-1-002.pdf.

[26] 15 U.S.C. § 1681 *et seq.*

[27] 42 U.S.C. § 3601 *et seq*.

encouraging consultation with regulators and requiring robust risk management, including appropriate testing, monitoring, and controls.[28]

The above-described activities are subject to *extensive* audit requirements and unique regulatory supervision. Banking organizations are required to have an independent internal audit system subject to board-level oversight, including for cybersecurity audits.[29] Prudential examiners assign ratings on banks' information security and audit programs, identify deficiencies that must be remedied, work with management to obtain corrective action, and pursue enforcement related to their findings as necessary.[30] For example, regulators conduct exams related to information security that must address topics such as governance, policies, and security controls and may include on-site reviews of independent testing of the bank's cybersecurity (e.g., penetration testing).[31] Examiners also assess the quality and independence of banks' internal audits, as well as conducting audit validation that may include verification procedures.[32]

As discussed above, banking organizations apply their governance processes and their federally required cyber audit, risk assessment, and model risk management activities across both their GLBA and FCRA data and data that is not subject to these frameworks. Accordingly, regardless of the statutory GLBA and FCRA exemptions, banking organizations will apply the above requirements to personal information subject to the CCPA.

III. The Proposal Exceeds the Agency's Limited Statutory Authority and Conflicts with the Primacy of the Federal Prudential Regulators.

The Agency does not have blanket authority to regulate cyber audits, risk assessments, and ADMT beyond its limited statutory grant of rulemaking authority, and, in particular, it does not have authority to regulate data that falls within the statutory exemptions, such as those for data subject to GLBA or FCRA. Moreover, the Agency must ensure that its regulations do not interfere with the primacy of prudential regulators' authorities under existing financial services laws. The Agency must conform its draft regulations to its statutory authority and the federal framework. Consequently, the Agency should make necessary revisions to various rule provisions, as set out in the appendix, and create an entity-level exemption from all three sets of rules for banking organizations.

a. The Proposed Rules Overstep the Agency's Rulemaking Authority.

The Agency has been given a limited statutory mandate for its rulemaking in these three areas. It may issue regulations requiring cyber audits and risk assessments for businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" and regulations "governing access and opt-out rights with respect to business's use of automated decisionmaking technology."[33] The Agency does not have blanket authority to regulate information

[28] BOARD, CFPB, FDIC, NCUA, & OCC, INTERAGENCY STATEMENT ON THE USE OF ALTERNATIVE DATA IN CREDIT UNDERWRITING (2019), *available at* https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-142a.pdf.

[29] Interagency Guidelines Establishing Standards for Safety and Soundness at Section II.B; *see also* Comptroller's Handbook at 35–36.

[30] Information Security Booklet at 74; *see also* 12 U.S.C. § 1818(b) (outlining procedure for a cease-and-desist order against a bank). These examinations are based on standards set forth in the Federal Financial Institutions Examination Council's Information Technology Examination Handbook ("IT Handbook").

[31] Information Security Booklet at 60–61.

[32] Audit Booklet at A-1–A-17; Comptroller's Handbook at 2.

[33] Cal. Civ. Code. § 1798.185(a)(15)–(16).

security, cyber audits, and risk assessments where there is no significant risk, including in the context of banking organizations that are already subject to prudential regulation that covers these activities. The Agency's new rules need to be firmly tethered to its existing authority, including in the following areas:

ADMT. The Agency does not have authority under the CCPA to regulate technology and artificial intelligence broadly. Overreach in this area is particularly inappropriate given that the California legislature and Governor are actively considering the most appropriate way to regulate artificial intelligence ("AI"). As Governor Newsom noted this fall when vetoing the legislature's AI safety bill, SB 1047, any AI governance solution should be "informed by an empirical trajectory analysis of AI systems and capabilities," and it is not appropriate to apply "stringent standards to even the most basic functions" of AI without consideration of key factors like whether the AI system is deployed in a high-risk environment or involves critical decision-making.[34] The Agency does not have the authority to address AI generally and must not usurp the legislature's role in crafting broad frameworks for governing AI.

Likewise, it is improper for the Agency to use its privacy authority to dictate how automation should be used in the context of employment and compensation decisions, given that other California regulators are specifically considering the regulation of automated decision systems in hiring, promotions, and other employment decisions.[35] For example, in § 7221(b)(3), the Agency conditions certain exemptions for ADMT in the employment context on policies, procedures, and training to protect against discrimination in the workforce. However, there are federal and state frameworks that are *designed* to address these risks. It would be far more appropriate to allow these agencies with expertise around employment to regulate this area.

Further, the CCPA framework does not authorize the Agency to adopt new rules for technologies that are not involved in making *decisions relating to consumers*. Thus, the Agency does not have authority to regulate extensive profiling and training of technologies – just the processing of personal information using an automated tool to make a decision relating to that consumer.[36] Members of the Agency's own Board – including Mr. Mactaggart, who was heavily involved in the drafting of the CCPA – have identified these provisions as "statutory overreach." In the context of risk assessments, for example, he noted that the Agency's scoping goes beyond the statutory "significant risk" standard by improperly focusing on the technology involved in the activity, rather than the nature of the activity.[37]

As another example, the Agency does not have authority to create consumer rights for a broad concept of "behavioral advertising" that appears to include first-party advertising, given the underlying CCPA framework specifically defines and addresses rights for "cross-context behavioral advertising." The regulation of first-party advertising is not consistent with the overall CCPA design, which is focused on affording consumers rights in the context of *sharing* personal information with third parties in certain defined circumstances.

[34] Letter from Gavin Newsom, Gov., to Members of the California State Senate (Sept. 29, 2024), *available at* https://www.gov.ca.gov/wp-content/uploads/2024/09/SB-1047-Veto-Message.pdf.

[35] *See, e.g.*, California Civil Rights Council, First Modifications to Initial Text of Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems (Oct. 4, 2024), *available at* https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2024/10/First-Modifications-to-Text-of-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf.

[36] Importantly, the CCPA protects only "consumers," i.e., "a natural person who is a California resident." Cal. Civ. Code § 1798.140(i). The Agency's final rules must not create any ambiguity that they apply to automation in relation to business customers, as opposed to consumers.

[37] Webcast of California Privacy Protection Agency Board Meeting (Nov. 8, 2024), *available at* https://cppa.ca.gov/meetings/materials/20241108.html.

As described in greater detail in Sections IV and the appendix, BPI recommends various changes to conform the proposed rules to the Agency's statutory authority relating to ADMT tools, including in the following areas:

Cybersecurity Audits. The Agency only has authority to create provisions on *audits*, yet it seeks to craft a cybersecurity control framework by requiring businesses to justify why they do not deploy *any single tactic* from a five-page, excessively prescriptive list of cybersecurity measures. This effectively forces businesses to deploy the enumerated tactics, even when they are duplicative or less protective than existing approaches. As outlined in Section IV, BPI recommends several changes to conform the proposed rules to the Agency's statutory authority relating to cyber audits.

Statutory Exemptions. The statutory design of the CCPA sought to avoid interference with federal regulation, including through exemptions for data subject to federal financial privacy frameworks, such as GLBA and FCRA.[38] As a result, there are real questions about whether the Agency has authority under the CCPA to impose significant new regulations on how banks, and other entities whose data is largely exempt from the CCPA, manage cybersecurity audits or other enterprise processes affected by the proposed rules.

At a minimum, the Agency does not have authority to impose backdoor regulation on data subject to GLBA via regulations that can only be satisfied via enterprise-wide compliance processes. This forecloses application of new enterprise cyber security processes on banking organizations that already apply the extensive existing financial regulatory framework across both GLBA and CCPA data and are already subject to federal supervision of these activities as discussed in Section II. In addition, while data subject to GLBA remains exempt pursuant to the underlying CCPA framework, the ADMT and risk assessment regulations contemplate regulation of decisions, and thus the underlying technology and systems leading to the decisions, without considering the classification of the data within these ADMT systems. This risks a practical overreach into data that is subject to GLBA, particularly as ADMT systems often are trained on and rely on a mix of GLBA and non-GLBA data. Accordingly, the Agency should more expressly clarify that its rules do not apply to technology that uses information governed by GLBA.

Likewise, the Agency does not have the authority to impose backdoor regulation on other data exempt from CCPA framework – such as protected health information subject to the Health Insurance Portability and Accountability Act ("HIPAA").

b. Even if the Agency Stayed Within Its Statutory Remit, the Proposed Rules Conflict In Part With the Primacy of Federal Prudential Regulation.

Even if the Agency made the above changes to more closely align with its statutory remit, its regulations would nonetheless conflict with the primacy of federal regulations for banking organizations – particularly national banks and federal savings associations.[39]

For national banks and federal savings associations, exclusive visitorial rights granted to the OCC by statute restrict the ability of states to inspect, examine, or regulate these entities' activities that are

[38] Cal. Civ. Code §§ 1798.145(a)(1) (exemption for compliance with laws), 1798.145(d), (e) (GLBA and FCRA exemptions).

[39] Title V of the GLBA includes a provision preserving state laws that are not inconsistent with its protections of customer information. *See* GLBA §§ 507, 524, codified at 15 U.S.C. §§ 6807, 6824. These preservation provisions, however, do not preclude a conclusion that a state law or regulation that purports to regulate the safety and soundness of banks' data usage practices is inapplicable to federally chartered institutions because it is inconsistent with the visitorial powers delegated to the OCC in the National Banking Act and the Home Owner's Loan Act or that such a state law is preempted by such Acts under the *Barnett* and *Cantero* standards.

authorized under federal banking law.[40] The applicability of certain elements of the Agency's proposed regulations to these institutions would violate the statutory prohibition against the exercise of visitorial authority over those institutions except as provided by federal law.[41] For example, under these authorities, California could not *directly* conduct the audits required by the regulations. It thus cannot achieve that result *indirectly* by purporting to require federally supervised banks to conduct an audit that addresses specific topics and certify completion to the state.[42] Likewise for risk assessments: California cannot force banks to conduct risk assessments that meet very specific requirements and then provide an abridged summary of (or, upon request, the full version of) each risk assessment. This type of direct inspection interferes with visitorial rights.

Accordingly, at a minimum, the Agency must eliminate the requirements to provide documentation to the Agency for banking organizations, as these requirements most plainly violate statutory prohibitions against the exercise of visitorial authority. These include the requirements to provide certifications of completion of cybersecurity audits under § 7124 and to provide documentation with respect to risk assessments under § 7157. These sections contemplate the provision of significant information about data processing activities and information security safeguards in conflict with federal law.

In addition, for national banks and federal savings associations, the three new proposed rules would be preempted since they would interfere with federally authorized banking activities.[43] As the Supreme Court has made clear, the applicability of state law to a national bank – that is, whether a state law is preempted – is determined by examining whether a state law 'prevents or significantly interferes' with the bank's conduct of a federally authorized activity. This principle was established in *Barnett*, codified by Congress in Dodd-Frank,[44] and recently upheld by the Supreme Court in *Cantero*.[45] Thus, the

[40] *See* 12 U.S.C. § 484. Visitorial powers are defined as (i) examination of a bank; (ii) inspection of a bank's books and records; (iii) regulation and supervision of activities authorized or permitted pursuant to federal banking law; and (iv) enforcing compliance with any applicable federal or state laws concerning those activities. Notably, examination of a bank's books and records is not limited to on-site inspection. *See* 12 C.F.R. § 7.4000. These requirements have been extended to federal savings associations and their subsidiaries. *See* 12 CFR § 7.4010(b).

[41] *See Barnett Bank of Marion County, N.A. v. Nelson*, 517 U.S. 25 (1996); 12 U.S.C. § 481 (documenting the OCC's authority to examine and require reporting from national banks); 12 U.S.C. § 484; 12 C.F.R. § 7.4000; 12 U.S.C. § 1465; and *Cuomo v. Clearing House Ass'n*, 557 U.S. 519 (2009).

[42] *See* Letter from Benjamin W. McDonough, Sr. Deputy Comptroller and Chief Counsel, Office of the Comptroller of the Currency to Chief Executive Officers of All National Banks and Federal Savings Associations, 1 n.3 (Nov. 9, 2023), *available at* https://www.occ.treas.gov/publications-and-resources/publications/banker-education/files/letter-to-chief-executive-officers.html. ("[T]o the extent that state laws purport to impose requirements such as attestation or reporting on national banks or FSAs, these laws may be inconsistent with the OCC's exclusive visitorial authority under federal law.").

[43] 517 U.S. 25 (1996). Under *Barnett*, which was codified for certain purposes by the Dodd-Frank Act, a court typically conducts a two-step analysis. First, the court determines whether the power or activity affected by the state law in question is authorized for national banks. Second, the court evaluates the degree of interference, or impact, the state law has on the national bank's exercise of the power. The court then draws a conclusion about whether the law is preempted. *See also Cantero v. Bank of Am., N. A.*, 602 U.S. 205, 221 (2024) (applying the *Barnett* standard).

[44] *See* Dodd-Frank Act section 1044(a), codified at 12 U.S.C. 25b(b).

[45] *See Cantero v. Bank of America, N.A.*, 144 S. Ct. 1290 (2024). Federal preemption applies to federal savings associations in the same way as it applies to national banks. Dodd-Frank Act section 1046, codified at 12 U.S.C. 1465.

Agency cannot adopt rules that interfere with the delivery of banking products and services, the use of technology to deliver those products and services, or other banking activities.[46]

Recently, the federal district court for the district of Illinois—citing *Cantero*, *Barnett*, and the prior Supreme Court cases relied upon in both of those decisions—preliminarily enjoined the State of Illinois from enforcing the Illinois Interchange Fee Prohibition Act ("IFPA") against national banks and federal savings associations on grounds of federal preemption.[47] Among other provisions, the court enjoined the state from enforcing the IFPA's provisions restricting banks' use of transaction data where that use is otherwise subject to federal regulation and supervision. As the OCC's briefs in the case explained, under well-established principles, federal law "cannot prevent or significantly interfere with a national bank's exercise of its federally authorized power to use and process transaction data."[48] Rather, this power should be interpreted broadly to avoid "preclud[ing] national banks' use of data in ways authorized by federal law to carry out the business of banking."[49]

The district court's determination that the IFPA provisions were preempted by federal law is instructive for purposes of the CCPA's rules. Here, as we have described above, the proposed rules interfere with the ability of national banks to deliver products and services to their customers in a way that is consistent with both the authorization to use technology in their businesses and the obligation of these institutions to do so consistent with federal safety and soundness standards. For example, the application of new rules impacting the training or use of ADMT in connection with banking products and services plainly interferes with the provision of bank products and services. Likewise, the application of lengthy and prescriptive risk assessment processes to bank activities interferes with those bank activities and therefore should be preempted. Further, the application of cybersecurity audit rules that are not aligned with existing requirements interfere with bank efforts to maintain cybersecurity safeguards to protect customer information.[50] To avoid interference with authorized activities, the proposed rules should not apply to national banks and federal savings associations. Moreover, because state-chartered banks are subject to nearly identical safety and soundness standards and requirements, they should receive similar treatment to national banks and federal savings organizations.

While BPI firmly believes these proposed rules should not be applicable to banking organizations for the reasons expressed throughout this letter, the Agency also should carefully consider significant

[46] National banks and federal savings associations are broadly authorized to use technology to deliver products and services so long as the means used are consistent with safety and soundness. 12 C.F.R. § 7.5000 (national banks); 12 C.F.R. Part 155 (federal savings associations).

[47] *Illinois Bankers Ass'n v. Raoul*, No. 24 C 7307, 2024 WL 5186840, at *7 (N.D. Ill. Dec. 20, 2024) (enjoining Illinois from applying key provisions of the IFPA to national banks and federal savings associations).

[48] Brief of the Office of the Comptroller of the Currency as *Amicus Curiae* In Support of Plaintiffs' Motion for a Preliminary Injunction at 15, *Illinois Bankers Association et al., v. Kwame Raoul*, Case No. 1:24-cv-07307 (N.D. Ill. Oct. 2, 2024) ("OCC Amicus Brief"). In contrast to the OCC, the Consumer Financial Protection Bureau – which is not the primary regulator of banks – has suggested in a non-precedential report that provisions in state privacy laws are not necessarily preempted by the National Bank Act. *See* CFPB, STATE CONSUMER PRIVACY LAWS AND THE MONETIZATION OF CONSUMER FINANCIAL DATA (Nov. 2024), *available at* https://files.consumerfinance.gov/f/documents/cfpb_state-privacy-laws-report_2024-11.pdf. However, as the OCC has made clear, there are complicated preemption issues to consider when regulating data in ways that would interfere with core banking activities. Indeed, preemption requires a specific inquiry for each power or activity affected by a state law.

[49] OCC Amicus Brief at 15.

[50] *See Watters v. Wachovia Bank, N.A.*, 550 U.S. 1, 22 (2007) ("[S]tate regulators cannot interfere with the 'business of banking' by subjecting national banks or their OCC licensed operating subsidiaries to multiple audits and surveillance under rival oversight regimes.").

security and competitive concerns that arise by concentrating a high volume of audit and risk assessment materials containing sensitive information. Taking on these types of risks could create litigation risk for the Agency.[51] Even for businesses other than banking organizations, the Agency's rules should require California regulators to maintain the confidentiality of these materials and the content within them and, to the extent the Agency creates limited circumstances where public disclosure is permissible, require that businesses are provided notice and an opportunity to object prior to any such disclosure.[52] Such confidentiality protections are consistent with the Agency's directive to prevent the disclosure of trade secrets.[53]

c. The Agency Can Avoid These Questions Through Targeted Exemptions For Banking Organizations Subject To Extensive Regulation.

To avoid conflict with the federal framework, the Agency should consider introducing appropriately scoped exemptions for banking organizations subject to prudential regulation. A narrowly crafted exemption for financial institutions that are subject to examination or supervision by a federal prudential regulator and their affiliates would avoid conflict with federal banking laws. Indeed, in including such exemptions, the Agency can rely on the fact that "[n]o other industry is subject to remotely comparable constraints and oversight."[54]

The frameworks described in Section II have been in place for many years and have protected personal information, as well as the broader integrity of the banking system. At best, the duplicative requirements in the draft rules would divert resources from promoting privacy and safeguarding our banking system in accordance with existing federal frameworks without corresponding benefit. At worst, they could disrupt the comprehensively regulated U.S. banking system without careful examination of the implications on that system or how the proposed rules might disrupt key consumer financial services. For example, the cybersecurity audit provisions risk interference with cybersecurity regulation for banking organizations, under which banking organizations already conduct rigorous, highly regulated cyber audits that are subject to layers of internal review and prudential supervision, even if such audits go beyond, and thus do not perfectly meet, each prescriptive requirement of the proposed cyber audit rules. And, as described in Section IV, the draft ADMT rules risk interference with how banking organizations use automated processes for a wide array of essential activities.

The Agency plainly has authority to create tailored exemptions from the new rules. The CCPA does not contain self-executing statutory provisions related to cybersecurity audits, risk assessments or automated decisionmaking. Rather, under CCPA § 1798.185, the Agency has discretion to adopt targeted rules that avoid interference with highly regulated industries and other regulatory frameworks. While the underlying statute crafted more narrow exemptions for personal information subject to GLBA and FCRA,

[51] *See* Declan Harty, *Dystopian surveillance, suspicionless seizures': Wall Street market monitor under attack*, Politico (Aug. 5, 2024), *available at* https://www.politico.com/news/2024/08/05/wall-street-new-chevron-challenge-00171627 (discussing numerous cases filed against the SEC related to its Consolidated Audit Trail, which similarly creates privacy and cybersecurity risk by condensing billions of sensitive trading records in one location).

[52] Notably, federal regulators treat audits and other examinations conducted under their jurisdiction as confidential; indeed, banking organizations are prohibited by law from disclosing the results of bank examinations performed by financial regulators given this is confidential supervisory information. OCC Bulletin 19-15: Supervisory Ratings and Other Nonpublic OCC Information: Statement on Confidentiality.

[53] *See* Cal. Civ. Code § 1798.185(a)(3).

[54] MORGAN RICKS, THE MONEY PROBLEM: RETHINKING FINANCIAL REGULATION (2016) (explaining that U.S. banking organizations "face detailed chartering criteria; strict limits on permissible activities […] extensive on- site supervision; [and] a vigorous enforcement regime").

the statutory framework directs the Agency to consider how to craft and scope regulations relating to cybersecurity audits, risk assessments, or automated decisionmaking. Indeed, the statute directs the Agency "to adopt regulations *to further the purposes of [the relevant] title*."[55] The statutory design of the CCPA sought to avoid interference with federal regulation of banking organizations, and so the Agency should similarly seek to avoid disrupting this regime through its new rules.

However, if the Agency does not include such an exemption, it will nonetheless need to make the changes discussed above to avoid exceeding its statutory authority and, in the case of documentation requirements, violating visitorial rights. Moreover, to avoid interference with essential banking activities and the complex patchwork of regulation and policy described above, the Agency will need to commit to carefully considering the impact of its new rules on the U.S. banking system, including by addressing the comments below in Sections IV, V, and VI.

IV. The ADMT Rules Require Clarification and Scoping To Avoid Undermining the Integrity of Various Banking Processes.

The Agency's draft ADMT rules – which read more like an artificial intelligence and technology governance framework than a privacy regulation – risk interfering with core banking processes, including compliance and safety and soundness activities. Should the Agency seek to regulate automated-decisionmaking without an exemption for banking organizations, it will be critical for it to consider how to appropriately scope and refine its rules to avoid disrupting essential banking activities.

a. Banking Organizations Have Long Used Automated Tools For a Wide Array of Essential Activities, Including Compliance and Safety and Soundness Processes, Under the Regulation and Supervision of Federal Regulators.

Banking organizations use automated processes for a wide array of essential activities, including underwriting and other lending activities, payment card processing, employment screening, and compliance processes. These are long-standing ADMT activities that banking organizations have conducted for many years. For example, as described above, banking organizations are governed by model risk management guidance and are supervised on its implementation and utilization, which has led to extensive dialogue with regulators including, in some cases, banks even being required to obtain pre-approval before adopting novel technology.[56]

The breadth of the proposed ADMT regulations and the lack of appropriate limitations on the requirements and rights created by the draft rules would impede these long-standing and common practices. For example:

- The rules risk limiting banking organizations' ability to use ADMT in certain underwriting and lending activities. Automated tools benefit the safety and soundness of banking organizations by increasing the underwriting and lending models' predictive capacity, thereby decreasing the likelihood a bank will be exposed to counterparty failure. For example, lenders may use models and algorithms to determine access to credit for small businesses, including sole proprietorships covered by the rules, because a bank may utilize inputs like the financial history of owners or guarantors.

[55] Cal. Civ. Code § 1798.185(a).

[56] *See generally* Model Risk Management Booklet. As previously mentioned, banking regulators subject banking organizations' use of emerging technology to excessive supervision, not insufficient oversight. Paridon, *supra* note 22.

- Additionally, given the inadequacy of the current security, fraud prevention, and safety exemption, the rules provide bad actors the capacity to weaponize opt-out rights to opt out of the application of critical fraud prevention tools that would be applied to their transactions and activities. Bank anti-fraud models may also grow less predictive and effective over time given that bad actors would also be able to opt out of their transactions and activities from being included as training data, meaning that these models would only be trained on a smaller subset of data for which there has not been an opt-out.

- As another example, lenders may rely on ADMT to identify, reach, or qualify prospective customers or applicants who are part of historically underserved populations, including those eligible for special lending programs to gain access to credit or credit terms not available under standard credit policies ("Special Purpose Credit Programs").[57] Moreover, in this context, federal regulators encourage lenders to deploy "affirmative advertising" to incentivize members of historically underserved groups or persons in underserved communities to apply for credit in accordance with the existing requirements of ECOA and Regulation B.[58] It is not clear the Agency has considered how the proposed ADMT regulations could undermine these efforts.

- Banking organizations also use ADMT models in connection with compliance processes that banks are required to conduct under federal, state, and local laws. For example, banks use automation to identify and report suspicious money laundering and terrorist financing activities; prevent parties that are subject to economic sanctions from accessing the U.S. banking system; review payment card transactions to complete chargebacks for challenged transactions; apply lending standards; and alert customers to account overdraft risk. While the CCPA makes clear that any ADMT obligations may not restrict a business' ability to comply with laws, the rules should expressly set forth that highly regulated banking organizations are not required honor opt-outs of ADMT that would inhibit compliance with these legal obligations.

- In order to protect depositors, banks must conduct employee screening under Section 19 of the Federal Deposit Insurance Act.[59] These employee screening processes could be subject to the regulations given the exceptionally broad definition of ADMT and somewhat narrow framing of the hiring exemption for opt-outs.[60] The FCRA already provides carefully calibrated notice obligations regarding adverse decisions and access and dispute rights, which could be undermined by the less calibrated rights in the draft rules. Moreover, the creation of notice and potentially opt-out rights for this process could provide applicants with information that could be used to circumvent the required screening process and thus increase the risk of insider fraud to depositors, or potentially allow applicants to opt-out of these required screenings and risk conflict with the operations banks undertake to comply with their Section 19 obligations.

[57] CFPB, COMMENT FOR 1002.4 – General Rules, Paragraph 4(b) *available at* https://www.consumerfinance.gov/rules-policy/regulations/1002/interp-4/.

[58] 12 C.F.R § 1002.8; Susan M. Bernard and Patrice Alexander Ficklin, *Expanding access to credit to underserved communities*, CFPB (July 31, 2020), *available at* https://www.consumerfinance.gov/about-us/blog/expanding-access-credit-underserved-communities/.

[59] 12 U.S.C. § 1829; 12 C.F.R. 303.220 *et seq.*

[60] Indeed, the draft regulations risk covering even use of standard software to assist in these processes, and the existing hiring exemption would seemingly not allow for software that has any use case beyond the "ability to perform at work."

Consumers rely on the availability of efficient and safe financial services products. BPI's members seek to provide these products in a privacy-protective manner, and the draft regulations could undermine banking organizations' ability to deliver products that consumers expect in a manner that minimizes fraud and safety risks. As Federal Reserve Governor Michelle Bowman recently noted, "customers are the ones who suffer" where "our regulatory environment is not receptive to the use of AI" for fighting fraud. As a result, "the regulatory system should promote these improvements [through AI tools] in a way that is consistent with applicable law and appropriate banking practices."[61]

In order to avoid interfering with these essential banking activities, the Agency must refine the scope and exemptions of its rules. Below, BPI outlines recommendations to help the Agency more appropriately scope its regulations to be privacy-protective while avoiding inadvertently undermining the banking system or creating additional questions about its authority.

b. The Agency Should Appropriately Scope the ADMT Definition and Regulations to Avoid Capturing Commonplace Uses of Automation and Software That Do Not Involve Decisionmaking.

The definition of "automated decisionmaking technology" in the regulations is extraordinarily broad and must be narrowed to cover only solely automated processing that produces legal and similarly significant effects concerning the consumer (consistent with other regimes).[62] As Board member Mr. Mactaggart has noted, the current ADMT definition results in the ADMT and risk assessment regulations "undermin[ing] privacy" in favor of "overreach, [a] lack of privacy protection, and [a] high likelihood of legal challenges."[63] Moreover, these regulations will waste business resources (particularly for entities like banking organizations that are already regulated in these areas), undermine socially beneficial uses of ADMT, and render the required risk assessments more a burdensome paperwork exercise than a meaningful tool for privacy supervision.

Indeed, as Mr. Mactaggart has observed, the CCPA does not contemplate regulation of essentially *any* computerized technology or software as ADMT – such as the example in the draft rules of a lone manager running a regression analysis in a spreadsheet. This example highlights both the Agency's overreach into regulating *any* technology (i.e., a spreadsheet) and the failure to appropriately scope the regulations (in line with comparable regimes) to exclude decisions made by humans, even where those humans may use ADMT outputs to facilitate their decision.

As discussed in Section III, it is also essential that the regulations are scoped to uses of ADMT resulting in a significant decision about a consumer, excluding any triggers related to profiling or training.[64] Further, the provisions addressing how businesses should handle opt-outs from ADMT should

[61] Speech by Gov. Michelle Bowman.

[62] *See, e.g.,* Regulation (EU) 2016/679, Art. 22. BPI recognizes that a minority of states have extended ADMT rules to automated processing that does not involve meaningful human engagement, *see, e.g.,* 4 Colo. Code Regs § 904-3 Rule 2.02 (discussing "Human Reviewed Automated Processing"). However, these other frameworks would regulate a much narrower scope of automation in other important respects, including applying only where technologies produce legal or similarly significant effects concerning a consumer and categorically exempting financial institutions. *See, e.g., id.* § 904-3 Rule 9.04(B); Colo. Rev. Stat. 6-1-1304(2)(q).

[63] Webcast of California Privacy Protection Agency Board Meeting (Nov. 8, 2024), *available at* https://cppa.ca.gov/meetings/materials/20241108.html.

[64] Were these triggers to be retained despite the open questions about the Agency's authority to regulate these uses of ADMT, the regulatory triggers for both ADMT and risk assessments related to profiling would need to be significantly revised to better align with existing frameworks. These regulations would need to be revised to focus

be clearly limited to the processing of personal information using ADMT for the purposes set forth in § 7200, consistent with the design of the proposed rules.

c. The Agency Should Ensure Robust Exemptions for Fraud and Security Incidents and Compliance Processes.

The Agency rightfully recognizes the importance of fraud prevention through the partial security, fraud prevention, and safety exemptions in the rules. However, the Agency's proposed exceptions must be revised in order to enable banking organizations and other industry participants in the U.S. banking system to protect consumers. For example:

- The exemption does not clearly cover fraud prevention activities conducted by banking organizations, which are often on behalf of third parties and not seeking to prevent fraud "directed at" only the business. For example, for payment card transaction processing, ADMT is most widely used to limit fraud, information security, and other risks *for cardholders, merchants, and other financial institutions.* The exemption similarly does not clearly protect banks' use of ADMT to resist illegal actions, such as money laundering and sanctions violations, that are "directed at" entities other than the bank (e.g., the federal government). While these exceptions do not, of course, limit the availability of the statutory exemption for compliance with laws, the creation of a partial exemption seems inconsistent with the underlying statutory exemption and warrants revision.

- Moreover, the exemption does not apply to the use of data for training ADMT models, despite the use of fraudsters' data being particularly essential to train models that are designed to catch subsequent fraudsters. Fraud models will become less effective over time when ingesting less information, particularly when the opt-outs may come in disproportionate numbers from fraudsters with an interest in undermining these processes.

- Even beyond the opt-out requirements, the notice and access requirements in § 7220 and § 7222 are problematic as applied to fraudsters, who could use information received to hone their fraud evasion strategies. For example, § 7222(b)(4) seems to contemplate that a banking organization would provide detailed information about how its algorithm identified the fraud, with a similarly inadequate fraud exemption in place. In addition, § 7222(k) would seemingly require that financial institutions inform fraudsters of their access right when denying a financial or lending service due to strong fraud signals, even where honoring that right could create serious issues for fraud prevention activities.

d. The Agency Should Provide A 24-Month Compliance Ramp Up Period.

Even if the above changes are implemented, these regulations will impose a substantial compliance burden. Businesses will have to assess the full universe of their existing ADMT technologies, collate extensive details about these technologies, and then build mechanisms to operationalize the new access and opt-out rights. Moreover, banking organizations will also have to consider how they can best comply in conjunction with federal regulation and supervision.

on *monitoring* of a publicly accessible place *on a large scale* (in alignment with General Data Protection Regulation ("GDPR") requirements for risk assessments); should not focus on work profiling, which is already covered by the triggers addressing significant work *decisions*; and to scope any requirements related to advertising to the advertising activity that the CCPA contemplates will be particularly regulated: *cross-context* behavioral advertising. *See, e.g.*, Regulation (EU) 2016/679, Arts. 22 and 35.

The Agency has already recognized that a 24-month period is appropriate to allow businesses to adequately complete cybersecurity audits and risk assessments for historic activities. Accordingly, BPI strongly recommends the introduction of an equivalent 24-month period for the ADMT regulations. This is particularly appropriate given the ongoing uncertainty about the scope of the final ADMT rules, including because of the Agency's disagreement with its Board about the scope of these rules, which has left businesses unable to even begin to prepare compliance strategies in the absence of final rules.

V. The Agency Must Ensure Cyber Audit Rules Do Not Interfere With Existing Frameworks For Managing and Auditing Financial Institution Cyber Risk

The contemplated cyber audits must be made more consistent with the frameworks used by banking organizations and their prudential regulators to address cyber risks. As discussed above, BPI recommends exempting banking organizations from the cyber audit rules in light of preexisting regulatory requirements. However, if the Agency nonetheless applies the requirements to banking organizations in some form, BPI recommends several revisions to the rules to help accomplish this goal, including language that clarifies that certain existing cybersecurity audit frameworks satisfy the requirements of the regulations, reduces the overly prescriptive nature of the regulations, and ensures that businesses may use internal auditors as well as external auditors.

a. Cyber Audit Requirements Should Be Harmonized With Existing Risk and Audit Frameworks.

Overly prescriptive cybersecurity audit regulations would directly undermine the Agency's stated policy goals. Both the federal financial regulatory agencies and widely accepted cybersecurity frameworks generally provide institutions with the flexibility to select cybersecurity measures appropriate for their unique risk profiles.[65] The more prescriptive approach proposed in the draft regulations will create unjustified inefficiencies at best and introduce risk for security systems at worst.[66] For example:

- Overly prescriptive regulations would conflict with existing audit practices, which often focus on previous deficiencies or elevated risks. Today, banking organizations conduct annual risk assessments and audit planning to allocate more audit resources for the highest risk entities and issues. In contrast, the draft regulations encourage a less effective one-size-fits-all audit approach that would restrict an institution's ability to deploy audit resources consistent with their internal risk assessments.

[65] *See, e.g.*, Interagency Guidelines Establishing Information Security Standards at Section III.C.1 ("Each national bank or Federal savings association *must consider* whether the following security measures are appropriate for the national bank or Federal savings association and, if so, adopt those measures the national bank or Federal savings association concludes *are appropriate* . . .") (emphasis added).

[66] BPI appreciates that the Agency has specified that the elements listed in the draft cybersecurity audit regulation must only be addressed "as applicable." However, the regulations nonetheless take an overly prescriptive approach in § 7123(b)(2) that requires businesses to justify why specific components are not necessary for their cybersecurity program and explain how its safeguards provide equivalent security. At a minimum, this will require businesses to expend unnecessary time, labor, and expense justifying why they don't rely on every prescriptive listed element. At worst, it could result in businesses – even those with limited presence in California and that process limited personal information that is subject to the CCPA framework – being effectively forced to implement cybersecurity protections that may be either unnecessary to, or in conflict with, elements of their holistic cybersecurity programs.

- Cybersecurity best practices are constantly evolving, and it is crucial that businesses maintain the flexibility to respond to new and emerging threats.[67] The prescriptive draft regulations would restrict businesses' ability to adapt to changing technology and require the Agency to constantly issue new regulations to keep pace with the evolving cybersecurity landscape. For example, the draft rules contemplate that audits will address "[s]trong unique passwords or passphrases," despite the fact that passwordless authentication is growing in adoption and is considered more secure than unique passwords. This type of requirement could perversely incentivize banks and other businesses to use less secure authentication means in order to reduce the burdens of their audits.

- The draft regulations also do not indicate whether an institution can satisfy the requirements through periodic audits, as opposed to one massive annual audit. This is inconsistent with the current practice of banking organizations which conduct multiple periodic audits over multiple entities and functions and processes within their institutions. Banking organizations determine the cadence of such cybersecurity audits based on their annual risk assessments. An institution can increase the audit frequency for an entity depending on risk at any time during the year, but a full annual audit might not be conducted for each individual process, function, or entity each year if there is minimal risk for that entity. Requiring banks to conduct a massive singular audit would impair and slow down the audit functionality of banking organizations and, for some organizations, be impossible given the breadth of their activities.

- Finally, the draft rules should be harmonized with widely accepted risk frameworks such as NIST CSF, the CRI Profile, frameworks governing banking organizations, and international frameworks promulgated under the GDPR. The draft regulations would not clearly allow for a cybersecurity audit against NIST CSF or the CRI Profile, which are flexible and non-prescriptive by design. These frameworks provide examples for achieving a desired outcome rather than mandating a "checklist of actions to perform" similar to those outlined in the draft rules.[68] For example, the NIST framework contains principles regarding access to assets that require managing risk "commensurate with the assessed risk."[69] However, even if a banking organization adequately addressed access controls under the NIST framework, the draft rules suggest that the institution might need to prepare a supplemental audit to address access rights granted to third party service providers via contract or explain why the business takes a minutely different approach to accomplish the same goal articulated in the draft rules.

To address the above issues, the regulations should specify that audits under comparable industry frameworks and recognized standards meet the requirements of the audit provisions. In addition, the Agency should adopt a less prescriptive approach that clarifies that specific cybersecurity measures must only be addressed where appropriate and allows for more general descriptions, as well as clarifying that multiple periodic audits may be used to comply with the statute and that an annual audit is not required in the absence of material changes or identified increased risk. The Agency should also moderate the thresholds for when an audit is required in recognition that these audits should only be required where there is a "significant" risk.

[67] *See* Improving the Nation's Cybersecurity, Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 17, 2021) (suggesting that the "private sector must adapt to the continuously changing threat environment"); Information Security Booklet at 13 (discussing the need to "review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors").

[68] NIST Cybersecurity Framework at 3.

[69] *Id.* at 19.

b. Cyber Audit Requirements Should Provide Greater Flexibility To Use an Internal Auditor.

While § 7122 of the proposed regulations facially permit using internal auditors, the specific requirements risk mandating an unrealistic level of independence that only an external auditor could achieve. For example:

- It is insufficiently clear what it means to have no "influence *by the business*" or not participate in any activity that "*may* compromise, *or appear to compromise*, the auditor's independence." While BPI understands this is not intended by the Agency, the language alone could be read to prohibit the business from employing the internal auditor.

- Most banks employ an audit structure where one chief auditor oversees a group of internal auditors and only that chief auditor reports to the board or an audit committee. This structure is seemingly impermissible under the draft requirements which could be read to require *every* auditor to directly report to the business's board. Moreover, in combination with the provisions that prohibit any "participat[ion] in the business activities," this requirement would likely prevent senior management from reviewing audit drafts prior to presentation to the board. This review is essential to ensuring the factual accuracy of the presentation and ensuring that senior management understands and can best respond to the audit findings.

- The draft regulations currently prohibit auditors from making recommendations regarding the business's cybersecurity program. Internal auditors frequently make observations as part of their audit reports that help improve a firm's cybersecurity posture. These observations could be impermissible under the draft regulations and would disincentivize auditors from making actionable observations. Moreover, within banking organizations, internal audit staff play an important role in keeping senior management updated on emerging risks. To the extent that discussions on emerging risks could be construed as "recommendations" or "particip[ation] in the business activities" under the regulation, the proposed rules would depress conversations that enhance cybersecurity by raising emerging issues for senior management proactively.

In contrast, the audits currently conducted by banking organizations meet the "thorough and independent" standard set forth in California law, without creating the above mentioned concerns.[70] The federal regulators require "independence and objectivity" and close oversight by the Board over "the effectiveness of the internal audit systems."[71] Internal auditors are required to "render impartial and unbiased judgments"; apply "independent judgment" when reviewing assessments conducted by other areas of the bank; and otherwise be "independent of the activities they audit so they can carry out their work freely and objectively."[72] The chief auditor – but not all internal auditors – also must report directly and regularly to the bank's board or audit committee.[73] In addition, banks follow a "three lines of defense" model that includes an independent risk management function below the internal audit function

[70] Cal. Civ. Code § 1798.185(a)(15)(A).

[71] Interagency Guidelines Establishing Standards for Safety and Soundness at Section II.B; *see also* Audit Booklet at 6; Comptroller's Handbook at 27.

[72] Comptroller's Handbook at 2, 24–27, and 35–36.

[73] *Id.* at 35; Audit Booklet at 6–7.

to oversee frontline business units that assess and manage risk. This provides the internal audit function with two degrees of separation from the frontline business units.

Finally, requiring banking organizations to use external auditors under the proposed regulations could lead to external auditor shortages. There is a limited pool of qualified third-party auditors, which banks must also use for purposes other than cybersecurity, such as financial audits. Once a bank uses an external auditor for a financial audit, that auditor is typically conflicted from conducting other activities on behalf of the firm. Because the pool of external auditors is so limited, banks could face significant compliance challenges as they attempt to balance complying with the regulations without violating these important conflict of interest rules. Indeed, in November 2022, the Federal Trade Commission delayed the enforcement of its revised Safeguards Rule due to a shortage of qualified personnel to implement the Rule's requirements.[74] Rather than risking a similar enforcement delay, the Agency should revise the regulations to more clearly allow for both internal and external auditors.

VI. Risk Assessment Rules Should Avoid Duplication and Ensure Interoperability with Other Frameworks.

The Agency should not require duplicative risk assessments where businesses already perform comparable risk assessments and should harmonize any supplemental requirements with existing privacy and cyber frameworks. Currently, the Agency's draft rules are poorly aligned with other sources of law – including both the federally required assessments described in Section II and other risk assessment procedures in international frameworks like the GDPR – and thus risk creating additional or redundant processes that will divert internal privacy resources without benefit to consumers. In order to address this, BPI strongly recommends clarifications to ensure that businesses can rely on risk assessments prepared to address other frameworks that *reasonably* address the prescriptive requirements in the regulations.

In addition, the Agency must consider the following essential revisions:

- The scope of these regulations should be narrowed (consistent with comparable regimes) to avoid overwhelming the Agency with a deluge of low-quality risk assessments that do not further the goals of the CCPA. Under the draft rules, the threshold for conducting risk assessments is misaligned with existing risk assessment frameworks that have a similar "significant risk" standard. For example, the European Data Protection Board's *Guidelines on Data Protection Impact Assessment* ("EDPB Guidelines") requires an assessment – consistent with the GDPR – only where processing is "likely to result in a high risk to the rights and freedoms of natural persons."[75] This includes "[a]utomated-decision making with legal or similarly significant effect" while excluding "[p]rocessing with little or no effect on individuals."[76] In contrast, the draft risk assessment regulations define "significant risk" to include many ADMT activities without consideration of whether a given activity presents significant risk. This will force businesses to focus on churning out duplicative assessments for run-of-the-mill technologies that have been in

[74] Press Release, FTC Extends Deadline by Six Months for Compliance with Some Changes to Financial Data Security Rule (Nov. 15, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-extends-deadline-six-months-compliance-some-changes-financial-data-security-rule.

[75] EUROPEAN DATA PROTECTION BOARD, GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND DETERMINING WHETHER PROCESSING IS "LIKELY TO RESULT IN A HIGH RISK" FOR THE PURPOSES OF REGULATION 2016/679, at 8–14 (April 4, 2017), *available at* https://ec.europa.eu/newsroom/article29/items/611236 ("EDPB Guidelines"); Regulation (EU) 2016/679, Art. 35.

[76] EDPB Guidelines at 9. Similarly, other state comprehensive privacy laws are more precisely scoped to require assessments for processing activities that present a *heightened risk of harm*. *See, e.g.*, Colo. Rev. Stat. § 6-1-1309.

use for many years, rather than conducting thoughtful assessments for activities that present a genuine significant risk to consumer privacy.

- The requirements for risk assessments in § 7152(a) should also be adjusted to be less prescriptive. Comparable regimes require a weighing of benefits and risks (as mitigated by safeguards) without imposing requirements to record details that may or may not be relevant to a particular data processing activity. In contrast, the more prescriptive requirements in the rules – such as the requirement in § 7152(a)(1) to avoid generic terms in describing the purpose of processing and the various ADMT-specific requirements – will be resource intensive without corresponding benefits. Indeed, these types of requirements could require reworking of existing risk assessment frameworks with a track record of effectiveness and decrease consistency with historical risk assessments.

- The Agency should also clarify that risk assessments are required only for new or genuinely materially different processing activities. As an initial matter, the requirement in § 7155(c) to conduct risk assessments *for all historical activity* that would be covered by the rules imposes an enormous compliance burden on businesses without any corresponding consumer benefit. For example, for banking organizations, longstanding Bank Secrecy Act ("BSA"), Anti-Money Laundering ("AML"), and Know Your Customer ("KYC") programs, small business lending, cybersecurity, and anti-fraud programs all require the processing of sensitive information and have been actively risk assessed, audited and examined for decades. Banking organizations will be forced to conduct a massive audit of all these data processing activities and to re-do their risk assessments even for activities that have been in place for many years without negative impacts to consumer privacy. This is not feasible within a 24-month period, let alone a desirable use of privacy resources.

  Looking forward, the requirement in § 7155(a)(3) to "immediately" update risk assessments where there is a "material change" is similarly unrealistic, given that a proper risk assessment requires careful collection and assessment of information. Moreover, the examples of material changes in the draft rules (presumably inadvertently) risk suggesting that even non-material changes to individual aspects or safeguards could require an updated risk assessment (e.g., there is a non-material change to one "purpose of the processing").

VII. Conclusion

To sum, the Agency's proposed rules risk interfering with core banking activities that are essential to the safety and soundness of the banking system, disrupting fraud prevention activities that benefit consumers and merchants, and undermining other important public policy goals that federal and state prudential regulators have spent years addressing. At a minimum, the Agency must revise its rules to avoid overstepping its authority by regulating data that is subject to GLBA or by regulating activities over which the CCPA does not grant it rulemaking authority (e.g., artificial intelligence). The Agency should also consider creating exemptions from these rules for banking organizations to most cleanly avoid these issues and infringement on federal primacy. In the absence of such exemptions, BPI has identified additional needed changes to all three sets of rules, including to allow for existing cybersecurity audits and risk assessments that are substantially similar to satisfy the requirements of the draft rules, ensure harmonization with the frameworks with which banking organizations already comply, and ensure robust exceptions for fraud, security, and other compliance activities.

* * *

The Bank Policy Institute appreciates the opportunity to submit these comments to the California Privacy Protection Agency on its rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking under the California Consumer Privacy Act. If you have any questions, please contact the undersigned by phone at (202) 589-2534 or by email at Joshua.Smith@BPI.com

Respectfully submitted,

/s/ Joshua Smith

Joshua Smith
Vice President, Assistant General Counsel
Bank Policy Institute

Appendix: Recommendations

Below we have set out several recommendations corresponding to each of the listed sections below. Sometimes we recommend revising one provision in several ways. For purposes of clarifying the reasons for each edit, we have organized recommendations by topic area rather than by provision. Nevertheless, we recommend that the Agency implement ***each*** edit to the relevant provision (e.g., we recommend that #7 and #24 both be implemented for § 7120(b)).

Section III.a. The Proposed Rules Overstep the Agency's Rulemaking Authority		
Recommendation Number	**Recommended Change**	**Recommended Text**
#1	Deletion or revision of § 7150(b)(3)(B)	*The reference to "extensive profiling" in § 7150(b)(3) and the entirety of § 7150(b)(3)(B) should be deleted, but if it is retained it should be revised, including as follows:* "For purposes of this Article, "extensive profiling" means any of the following to the extent the relevant observation or profiling involves systematic use of information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5):"
#2	Deletion or revision of § 7150(b)(4)	*§ 7150(b)(4) should be deleted in its entirety, but if it is retained it should be revised, including as follows:* "Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence ~~that is capable of being~~ that is designed to be used for any of the following (but excluding the processing of personal information that is subject to, or the training of automated decisionmaking that is designed to be used with personal information that is subject to, one or more exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5)):"
#3	Revision of § 7200(a)	"A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article, provided that this Article shall not apply to use of automated decisionmaking technology in contexts in which data collected would be subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5): . . . "

#4	Deletion or revision of § 7200(a)(2)	*§ 7200(a)(2) should be deleted in its entirety, but if it is retained it should be revised, including as follows:* “For extensive profiling of a consumer. For purposes of this Article, “extensive profiling” means any of the following to the extent the relevant observation or profiling involves systematic use of information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5):”
#5	Deletion or revision of § 7200(a)(3)	*§ 7200(a)(3) should be deleted in its entirety, but if it is retained it should be revised, including as follows:* “~~For training uses of automated decisionmaking technology, which are p~~Processing consumers’ personal information to train automated decisionmaking technology ~~that is capable of being~~ that is designed to be used for any of the following (but excluding the processing of personal information that is subject to, or the training of automated decisionmaking that is designed to be used with personal information that is subject to, one or more exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5)):”
Section III.c. The Agency Can Avoid These Questions Through Targeted Exemptions For Banking Organizations Subject To Extensive Regulation		
Recommendation Number	**Recommended Change**	**Recommended Text**
#6	Addition of §§ 7120(c), 7150(d), and 7200(b)	“This Article [9, 10, or 11] does not apply to financial institutions that are subject to examination or supervision by a federal prudential regulator and their affiliates as defined under the Bank Holding Company Act, 12 U.S.C. § 1841(k).”
#7	In the alternative, revision of § 7120(b)	“A business’s processing of consumers’ personal information presents a significant risk to consumers’ security if the business is not subject to examination or supervision by a federal prudential regulator with respect to cybersecurity and any of the following is true:”
#8	In the alternative, revision of § 7124(a) and § 7157(b)(4)	“Each business that is required to complete a cybersecurity audit pursuant to this Article must submit to the Agency every calendar year a written certification that the business completed the cybersecurity audit as set forth in this Article unless the business is subject to examination or supervision by a federal prudential regulator with respect to cybersecurity.”

		“A business is not required to submit a risk assessment to the Agency if the business does not initiate the processing activity subject to the risk assessment or if a risk assessment is undertaken in a manner that is subject to examination or supervision by a federal prudential regulator.”
#9	In the alternative, addition of § 7124(d) and § 7157(e)	“This [§ 7124][§ 7157] does not apply to financial institutions that are subject to examination or supervision by a federal prudential regulator and their affiliates.”
#10	In the alternative, revision of § 7150(b)	“Each of the following processing activities presents a significant risk to consumers except to the extent undertaken in a manner that is subject to examination or supervision by a federal prudential regulator:”
#11	In the alternative, revision of § 7200(a) and addition of new § 7200(b)	“A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article except as set forth in subsection (b) below:” In addition, a new § 7200(b) would be added as follows: “Automated decisionmaking technologies that are subject to examination or supervision by a federal prudential regulator are not subject to the requirements of this Article.”

Section IV.b. The Agency Should Appropriately Scope the ADMT Definition and Regulations to Avoid Capturing Commonplace Uses of Automation and Software That Do Not Involve Decisionmaking

Recommendation Number	Recommended Change	Recommended Text
#12	Revision of § 7001(f), including deletion of 7001(f)(1)-(4)	“‘Automated decisionmaking technology’ or ‘ADMT’ means any ~~technology that processes~~ solely automated processing of personal information ~~and uses computation~~ to execute a decision which produces legal or similarly significant effects ~~or replace human decisionmaking, or substantially facilitate human decisionmaking~~.” or, *in the alternative:* “‘Automated decisionmaking technology’ or ‘ADMT’ means any ~~technology that processes~~ solely automated processing of personal information ~~and uses computation~~ to execute a decision or replace human decisionmaking~~, or substantially facilitate human decisionmaking~~.”

		In addition, the defined term “artificial intelligence” should be deleted in § 7001(c).
#13	In the alternative, revision of § 7001(f)(4)	“Automated decisionmaking technology does not include the following technologies~~, provided that the technologies do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking~~: web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam-and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies. A business must not use these technologies to circumvent the requirements for automated decisionmaking technology set forth in these regulations. For example,~~ a business’s use of a spreadsheet to run regression analyses on its top-performing managers’ personal information to determine their common characteristics, and then to find co-occurrences of those characteristics among its more junior employees to identify which of them it will promote is a use of automated decisionmaking technology, because this use is replacing human decisionmaking. By contrast~~, a manager’s use of a spreadsheet to input junior employees’ performance evaluation scores from their managers and colleagues, and then calculate each employee’s final score that the manager will use to determine which of them will be promoted is not a use of automated decisionmaking technology, because the manager is using the spreadsheet merely to organize human decisionmakers’ evaluations.”
#14	Deletion of § 7150(b)(3)(B), § 7150(b)(4), § 7200(a)(2), and § 7200(a)(3), as well as the reference to “extensive profiling” in § 7150(b)(3)	*These provisions should be deleted in their entirety.*
#15	Revision of § 7200(a)	*The following revision should be made to definitively ensure that the rules do not create any ambiguity that they apply to automation in relation to business customers, as opposed to consumers:* “A business that uses automated decisionmaking technology to make decisions about natural persons who are California residents in any of the following ways must comply with the requirements of this Article: . . . ”

#16	Addition of § 7200(b) or (c)	“Businesses shall not be required to audit individual employees’ activities for whether they are using ADMT for the purposes listed in § 7200(a).”
#17	Revision of §§ 7221(m) and (n), including deletion of 7221(n)(2)	“If the consumer submits a request to opt-out of ADMT before the business has initiated that processing, the business must not initiate processing of the consumer’s personal information for the purposes set forth in section 7200, subsection (a) using that automated decisionmaking technology.” “If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out of ADMT after the business initiated the processing, the business must comply with the consumer’s opt-out request by: (1) Ceasing to process the consumer’s personal information for the purposes set forth in section 7200, subsection (a) using that automated decisionmaking technology as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. ~~For personal information previously processed by that automated decisionmaking technology, the business must neither use nor retain that information; and~~”
Section IV.c. The Agency Should Ensure Robust Exemptions for Fraud and Security Incidents and Compliance Processes		
Recommendation Number	**Recommended Change**	**Recommended Text**
#18	Addition of § 7220(b)	“A business is not required to comply with this Article 11 where such compliance would (a) compromise its use of automated decisionmaking technology for security, fraud prevention, or safety purposes or (b) compromise processes used to comply with laws to which the business is subject.”
#19	Revision of § 7221(b)(1)	“A business is not required to provide consumers with the ability to opt-out of a business’s use of automated decisionmaking technology ~~for a significant decision concerning a consumer as set forth in section 7200, subsection (a)(1); for work or educational profiling as set forth in section 7200, subsection (a)(2)(A); or for public profiling as set forth in section 7200, subsection (a)(2)(B),~~ in the following circumstances: (1) The business’s use of that automated decisionmaking technology is for ~~necessary to achieve, and is used solely for, the~~ security, fraud prevention, or safety purposes, including but not limited to the 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 or the availability, integrity, or confidentiality of information systems, or otherwise help ensure security and integrity of personal information or information systems; (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; (D) To otherwise ensure security and integrity; or (E) To comply with laws, including any regulation or guidance implementing such laws." *Note that "security and integrity" is already defined in the CCPA. In addition, conforming changes should be made elsewhere, including striking references to "direct at the business" in §§ 7027(m)(3) and 7157(b)(2)(D). In addition, comparable changes should be made to similar language in the regulations, such as § 7157(b)(2)(D).*
#20	Revision of § 7221(b)(3)	*The Agency should also consider more appropriately scoping the other exemptions in its ADMT rule:* "For admission, acceptance, or hiring decisions as set forth in section 7200, subsections (a)(1)(A)(i), (a)(1)(B)(i), if the following are true: (A) The automated decisionmaking technology is for ~~necessary to achieve, and is used solely for,~~ the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and . . . " *Corresponding revisions should be made to § 7221(b)(4) and (b)(5).*
#21	Revision of § 7221(b)(6)	Deletion of this provision or "The exceptions in this subsection do not apply to profiling for behavioral advertising as set forth in section 7200, subsection (a)(2)(C)~~, or to training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3)~~. A business must provide the ability to opt-out of these uses of automated decisionmaking technology in all circumstances."
#22	Revision of § 7221(g)	*The Agency must revise this provision to avoid forcing businesses to provide information to bad actors that they can use to further fraudulent activities:*

		“If a business has a good-faith, reasonable, and documented belief that a request to opt-out of ADMT is fraudulent, the business may deny the request. The business must inform the requestor that it will not comply with the request ~~and must provide to the requestor an explanation why it believes the request is fraudulent~~.”
Section IV.d. The Agency Should Provide A 24-Month Compliance Ramp Up Period		
Recommendation Number	**Recommended Change**	**Recommended Text**
#23	Addition of § 7200	“For any use of automated decisionmaking technology identified in section 7200(a) that the business initiated prior to the effective date of these regulations and that continues after the effective date of these regulations, the business must comply with the requirements of this Article 11 within 24 months of the effective date of these regulations.”
Section V.a. Cyber Audit Requirements Should Be Harmonized With Existing Risk and Audit Frameworks		
Recommendation Number	**Recommended Change**	**Recommended Text**
#24	Revision of § 7120(b)(2)	“(2) The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A); and (A) Processed the personal information of 500,000 ~~250,000~~ or more consumers or households in the preceding calendar year; or (B) Processed the sensitive personal information of 250,000 ~~50,000~~ or more consumers in the preceding calendar year.”
#25	Revision of § 7121(b)	After the business completes its first cybersecurity audit pursuant to subsection (a), its subsequent cybersecurity audits must be completed regularly, such as at least once every calendar year~~, and there must be no gap in the months covered by successive cybersecurity audits~~. *Conforming changes should be made elsewhere where “annual” is referenced, including to § 7124 to require that the written certification describe the period covered by the most recent audit.*

#26	Revision of § 7123(a)	"The cybersecurity audit must assess and document how the business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information. This audit may be conducted using multiple audits, provided that the below requirements are satisfied across these audits."
#27	Revision of § 7123(b)(2)	"The cybersecurity audit must specifically identify, address, and document . . . Each of the following components of the business's cybersecurity program, as applicable and appropriate to the business's size and complexity and the nature and scope of its processing activities**.** If not applicable, the cybersecurity audit must document and explain any comparable components relevant to the business's protection of personal information ~~why the component is not necessary to the business's protection of personal information and how the safeguards that the business does have in place provide at least equivalent security~~." *In addition, the Agency should undertake a careful review of the listed components in order to revise them to be more general and thus more future proofed. For example, the requirement in § 7123(b)(2)(A) should be limited to "authentication" as opposed to specific mechanisms for authentication (e.g., strong unique passwords which are already becoming out-of-date).*
#28	Revision of § 7123(b)(3)	"For each of the applicable components set forth in subsections (b)(1)–(2), including the safeguards the business identifies in its policies and procedures, the cybersecurity audit must describe how the business implements and enforces compliance with them. This description may be either general or specific to each of the requirements."
#29	Addition of § 7123(g)	"If a business identifies and documents that there have been no material changes to the components outlined in § 7123(c) for a given entity or line of business during a period, then the business shall not be required to complete a cybersecurity audit that meets all of the requirements of § 7123 in that period, provided that the business must conduct a cybersecurity audit that meets all of the requirements of § 7123 for that entity or line of business at least once every three years."
#30	Addition of § 7120(c) and § 7120(d)	"A business will be deemed to be in full compliance with this Article 9 if it completes a cybersecurity audit, assessment, or evaluation that complies with the requirements of the Federal Financial Institutions Examination Council's IT Examination Handbook, the Gramm-Leach-Bliley Act, or the New York Department of Financial Services' Cybersecurity Regulation." and

		“Any cybersecurity audit, assessment, or evaluation conducted against any list of approved frameworks promulgated by the California Privacy Protection Agency shall be considered to meet the requirements of this Article 9. The approved frameworks shall include: the National Institute of Standards and Technology’s (“NIST”) Cybersecurity Framework and successor frameworks released by NIST, the Cyber Risk Institute Profile and successor frameworks, and those audits, evaluations, and examinations conducted by or under the supervision of federal prudential regulators.”

V.b. Cyber Audit Requirements Should Provide Greater Flexibility To Use an Internal Auditor

Recommendation Number	Recommended Change	Recommended Text
#31	Revisions to § 7122(a), including deletion of § 7122(a)(1) and (2)	“Every business required to complete a cybersecurity audit pursuant to this Article must do so using a qualified, objective, independent professional (“auditor”) using procedures and standards generally accepted in the profession of auditing. The auditor may be internal or external to the business but shall be independent and objective. The business’s audit committee or board of directors shall be responsible for the effectiveness of the internal audit systems and shall receive regular reports on internal cybersecurity audit issues.”

VI. Risk Assessment Rules Should Avoid Duplication and Ensure Interoperability with Other Frameworks

Recommendation Number	Recommended Change	Recommended Text
#32	Revision of § 7152(a)	“The business must conduct a risk assessment to determine whether the risks to consumers’ privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing. The business must conduct and document the risk assessment ~~as~~ in accordance with the requirements set forth below, in each case where relevant to the identified significant risk to consumers’ privacy and security: . . . ”
#33	Revisions to § 7152(a)(1), 7152(a)(2), and 7152(a)(6) (among other revisions to decrease the	“The business must specifically identify its purpose for processing consumers’ personal information. ~~The purpose must not be identified or described in generic terms, such as ‘to improve our services’ or for ‘security purposes.~~’” “The business must identify the categories of personal information to be processed and whether they include sensitive personal information. This must include discussion of the following, as applicable:”

	prescriptive nature of the regulations)	“ . . . The business must identify the safeguards that it plans to implement to address the negative impacts identified in subsection (a)(5). The business must specifically identify how these safeguards collectively address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures.”
#34	Revision of § 7155(a)(3)	“Notwithstanding subsection (a)(2) of this section, a business must ~~immediately~~ update a risk assessment whenever there is a material change relating to the processing activity. A change relating to the processing activity is material if it diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4), creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6), in each case as material to the benefits, impacts, or effectiveness of the safeguards. Material changes may include, for example, material changes to the purpose of the processing; material changes **to** the minimum personal information necessary to achieve the purpose of the processing; or material changes to the risks to consumers’ privacy ~~raised by consumers (e.g., numerous consumers complain to a business about the risks that the business’s processing poses to their privacy)~~.”
#35	Revision of § 7155(c)	“For any processing activity identified in section 7150, subsection (b), that the business initiated prior to the effective date of these regulations and that continues after the effective date of these regulations, the business must conduct and document a risk assessment in accordance with the requirements of this Article where there is a material change to the data processing ~~within 24 months of the effective date of these regulations~~.”
#36	Revision of § 7156(b)	“If the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that reasonably meets ~~all~~ the requirements of this Article, the business is not required to conduct a duplicative risk assessment. If the risk assessment conducted and documented for the purpose of compliance with another law or regulation does not reasonably meet ~~all of~~ the requirements of this Article, the business may ~~must~~ supplement the risk assessment with any additional information ~~required~~ to meet ~~all of~~ the requirements of this Article.”
#37	Addition of § 7157(e)	*The Agency should (consistent with the grant of rulemaking authority in the CCPA) expressly clarify that the regulations do not require businesses to divulge trade secrets:* “Nothing in this Article 10 shall require a business to divulge trade secrets.”

From: Chris Micheli <cmicheli@snodgrassmicheli.com>
Sent: Friday, January 10, 2025 9:26 AM
To: Regulations@CPPA
Subject: FW: CPPA letter due Jan 14
Attachments: CPPA Letter.docx

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Chris Micheli
Snodgrass & Micheli, LLC
1121 L Street, Suite 807
Sacramento, CA 95814
(916) 743-6802
cmicheli@snodgrassmicheli.com

From: Esabella De La Caridad Rojas <ERojas@lachamber.com>
Sent: Thursday, January 9, 2025 4:51 PM
To: Chris Micheli <cmicheli@snodgrassmicheli.com>
Subject: CPPA letter

Hi Chris,
Here is the letter for the CPPA hearing January 14.
Thanks,
Esabella

Esabella Rojas | Public Policy Manager
LOS ANGELES AREA CHAMBER OF COMMERCE
350 S. Bixel St. | Los Angeles, CA 90017

P: 213.580.7518
erojas@lachamber.com | www.lachamber.com

A THRIVING REGION FOR ALL

LOS ANGELES AREA
CHAMBER OF COMMERCE

January 7, 2025

To: California Privacy Protection Agency

RE: Los Angeles Area Chamber of Commerce Opposition to Proposed Automated Decision Making Technology (ADMT) Regulations

To Whom It May Concern:

On behalf of the Los Angeles Area Chamber of Commerce, representing a broad spectrum of small and large businesses in the Los Angeles region, we are writing to express our strong opposition to the proposed automated decision making technology (ADMT) regulations. While the Chamber shares the agency's goal of strengthening consumer privacy, these regulations as written are overly broad, extend beyond the agency’s privacy mandate, and would impose substantial burdens on businesses that are out of proportion to any corresponding gains in consumer privacy. The agency should revise these rules to focus on the kinds of specific, meaningful privacy risks that motivated California voters to create the agency, rather than creating sweeping requirements that would regulate and hamper a swath of routine business operations across California.

At a high level, these regulations extend far beyond the reason voters, through Proposition 24, created the agency: to be an “independent watchdog whose mission is to protect consumer privacy.” Instead, they would create an expansive new regulatory framework that would capture and regulate even basic, decades-old technologies that businesses large and small use every day, even if these systems pose no meaningful (let alone significant) privacy risks. The proposed rules are so broad, and seek to regulate such a wide range of activities and policy areas, that they would be unrecognizable to the Californians who supported Proposition 24. The result is that, according to the agency's own analysis, these regulations could cost businesses $3.5 billion - and even this substantial figure likely understates the true economic impact.

The proposed regulations define automated decision-making technology so broadly that they would capture routine business tools like spreadsheets, basic database operations, and standard workplace monitoring systems, regardless of whether these tools meaningfully threaten consumers’ privacy. The proposed regulations say they do not mean to regulate those kinds of very basic technologies. But, in an exception that swallows that rule, the regulations go on to say that, in fact, everyday software like spreadsheets and databases are covered if they’re used to help a human make a decision, or even just “execute a decision” a human has already made. For example, the rules say that if a manager uses Excel to analyze employee performance data to factor that into routine pay or promotion decisions, these mundane operations would suddenly be subject to burdensome new auditing, disclosure, and opt-out requirements, no matter the fact that this kind of everyday activity poses no meaningful consumer privacy risks.

Additionally, the proposed regulations seek to regulate how businesses across the state use technology to help them make decisions across a wide range of topics, including lending, housing, education, employment, healthcare, and various consumer goods, without sufficiently connecting those regulations to the agency’s privacy mandate. The agency is a privacy regulator, not a housing regulator or an employment regulator (or even an automated-technology regulator), so the agency’s regulations must be narrowed to focus on business activities that carry genuine consumer-privacy risks.

Even though these regulations supposedly are focused on “automated decisionmaking” technologies,” they are not limited to the kinds of AI and other cutting-edge technology capable of making truly “automated” decisions without human oversight. Instead, they would apply to mainstream technologies that have been used safely and effectively for decades. The rules would require extensive documentation, risk assessments, and opt-out mechanisms even for basic softwares that simply help humans make decisions, rather than truly replace human judgment. This approach is dramatically out of step with other regulatory frameworks, which appropriately focus on truly automated systems that make decisions without meaningful human oversight, and this approach would impose major new burdens on systems that are already subject to human oversight and control.

The proposed rules would create significant competitive disadvantages for California businesses. The requirement to publicly disclose the "logic" and "key parameters" of a wide range of business systems could force companies to reveal trade secrets and proprietary information, despite the fact that the agency's governing laws specifically say that trade secrets should be protected. These disclosures also could provide bad actors with roadmaps to game or manipulate systems, potentially increasing fraud and harming all the rest of the consumers who are acting in good faith.

the regulations would severely restrict businesses' ability to engage in routine first-party advertising to their own customers. Currently, businesses can tailor their advertising and promotions based on customers' past purchases – like a grocery store sending coupons for baby food specifically to customers who have bought baby supplies in the past. These regulations would require any business engaging in this common practice to implement complex opt-out systems for personalized advertising. For many businesses, especially smaller ones, developing and maintaining such systems would be technically infeasible. Unlike existing regulations that focus on controversial third-party tracking across different websites, these rules would restrict how businesses communicate with their own customers about products and services they've already shown interest in purchasing. This would be an unnecessary expansion of privacy regulations into routine business practices that consumers generally find helpful, not harmful.

We strongly urge the agency to substantially revise these proposed regulations to focus on meaningful privacy risks while avoiding unnecessary burdens on California's business community. The current approach would create significant costs and complications while failing to effectively address the privacy concerns that motivated California voters to give the agency its mandate to adopt these rules. Please feel free to contact Esabella Rojas at erojas@lachamber.com, if you have any questions.

Sincerely,

[redacted]

Maria S. Salinas
President & CEO

From: Anthony Licon
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Date: Monday, January 13, 2025 2:48:39 PM

Dear Members of the CPPA,

I am the Chief Strategy Officer and partner of Epic Reach, LLC., an agency operating in Burbank, California. I am writing to express my serious concerns regarding the proposed regulations on cybersecurity audits, risk assessments, automated decision-making technology (ADMT), and insurance companies.

Our Business and the Services We Provide
We are a small business that provides digital services to an assortment of small and incumbent businesses, which rely on responsibly collected consumer data to efficiently enhance our offerings and provide value to our customers.

Among other things, the proposed regulations would a) require additional pre-use disclosures over and above existing transparency requirements, specific to ADMTs, *including for existing customers*; b) require opt-out mechanisms specific to ADMTs; c) require the disclosure of detailed information about ADMTs companies use, including “parameters that affect the output of the [ADMT].” There are three main reasons we oppose the proposed ADMT and risk assessment rules:

1. **The proposal would undermine our efforts to meet consumer expectations.** Privacy is about meeting expectations. The proposed rule would mandate disclosures about ADMTs for consumers that have already agreed to receive products and services, inserting additional digital red tape between customers and services they expect to receive.
2. **The rules would impose new costs without any commensurate privacy benefit for consumers.** CPPA’s own cost estimate forecasts direct costs of $31 billion, a net loss of 98,000 jobs, and a $27 billion gross state product loss from the proposed rules over the next 12 years. Much of this cost is unnecessary, especially since other CPPA rules already require companies to accommodate universal opt-out and must also respond to consumer requests related to privacy.
3. **The proposal would likely undermine privacy.** By saddling consumers with additional notices and screens—when further interruptions are totally unexpected—the

regulations would cause notice fatigue. This would serve to erode the trust people have in privacy notices generally, and without trust there cannot be a meaningful privacy dialogue.

The Disproportionate Impact on Small Businesses

Even worse, the proposal would pile on top of completed rulemakings, including the Delete Act regulations. The unprecedented increase in data broker registration fees in that rulemaking from $400 to $6,600 amounts to a staggering **1,550% increase**.

I am deeply concerned about the disproportionate financial burden this fee places on small businesses like mine. Unlike larger corporations, for whom $6,600 is a negligible expense, this dramatic increase presents a significant hurdle to our ability to operate, innovate, and grow. Similarly, the expansion of the definition of a "data broker" to include businesses that sell information collected indirectly from consumers, even those with whom a **"direct relationship"** exists, further complicates compliance.

By broadening the scope of what constitutes a data broker while simultaneously implementing an astronomical fee increase, the Delete Act regulations will create a regulatory environment that unfairly penalizes small businesses while allowing larger companies to absorb these costs with ease.

It is in this context that the ADMT and risk assessment proposals appear and only exacerbate already untenable compliance costs for small businesses.

I urge the CPPA to:

1. Withdraw all of the proposed regulations relating specifically to ADMTs and instead address the ADMT requirements as part of broader requirements that relate to privacy.
2. Reverse the Delete Act regulations that increase filing fees and unnecessarily expand the “data broker” and “direct relationship” definitions.
3. Engage more closely with small businesses during the regulatory process to ensure that our voices are heard, and our challenges are addressed.

Thank you for your time to read my concerns and consideration. I hope the agency considers the needs of small businesses like mine. It is imperative that CCPA’s requirements strike a more realistic balance between privacy and consumer protection for companies doing business in California.

Sincerely,
Anthony Licon

CSO
epic reach
4100 W Alameda Ave Suite 369
Burbank CA 91505

From:	Olga Medina <OlgaM@bsa.org>
Sent:	Tuesday, January 14, 2025 12:45 PM
To:	Regulations@CPPA
Cc:	Meghan Pensyl
Subject:	Business Software Alliance - Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance
Attachments:	BSA Comments on 2024 CPPA rules.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear Candice,

Attached, please find the Business Software Alliance’s written comments to the California Privacy Protection Agency’s proposed regulations on automated decisionmaking, cybersecurity audits, and risk assessments.

Thank you for the opportunity to provide input.

Best,
Olga

Business
Software
Alliance

January 14, 2025

The Business Software Alliance
Submission to the California Privacy Protection Agency
on Proposed Regulations on Automated Decisionmaking Technology, Cybersecurity Audits, and Risk Assessments

The Business Software Alliance (BSA) welcomes the opportunity to submit comments in response to the California Privacy Protection Agency's (CPPA) proposed rulemaking on automated decisionmaking, cybersecurity audits, and risk assessments ("the proposed regulations"). We appreciate the CPPA's work to address consumer privacy and its goal of issuing regulations that better protect consumer privacy.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, cybersecurity solutions, human resources management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We appreciate the proposed regulations' goal of increasing privacy for California consumers but have significant concerns with practical aspects of the current draft. We recommend changes to all three topics on which the CPPA seeks public comment:

1. ***Automated Decisionmaking***. The CPPA should clarify the scope of the proposed regulations on automated decisionmaking technology (ADMT) and revise how they work in practice. Specifically, the agency should clarify the definitions of ADMT and "significant decision"; reconsider provisions on training ADMT or AI; address implementation challenges for pre-use notices, opt-outs of ADMT, and requests to access ADMT; and harmonize the proposed ADMT regulations with other legislative and regulatory efforts on AI.

2. ***Cybersecurity Audits.*** The CPPA should adopt a flexible, risk-based, and harmonized approach to cybersecurity auditing requirements; specify that cybersecurity audits, certifications, and evaluations already performed by companies satisfy the California Consumer Privacy Act's (CCPA) requirements; remove the requirement that cybersecurity audits and issues raised in them should be reported to the business's board of directors; and define processing that presents a "significant risk" to consumers' security in line with leading cybersecurity laws, policies, and standards.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

3. ***Risk Assessments.*** Although BSA supports the use of risk assessments to identify and mitigate potential privacy risks, we are concerned with the approach to risk assessments set out in the proposed regulations. The CPPA should require fewer risk assessment materials be submitted to the agency; define processing that presents a “significant risk” to consumers’ privacy in line with other global and state privacy laws; and revise the content to be included in risk assessments.

I. Automated Decisionmaking

As leaders in the development of enterprise AI, BSA members have unique insights into the technology’s tremendous potential to further spur digital transformation in the private and public sectors and the policies that can best support the responsible use of AI, especially high-risk uses of AI.

BSA has long called for legislation addressing high-risk uses of AI, meaning when AI tools are used to make decisions that significantly impact consumers’ lives, which are often referred to as “consequential decisions.” BSA believes that in such contexts both AI developers, the companies that create AI systems, and AI deployers, the companies that use high-risk AI systems, should have obligations to protect against unlawful discrimination, including to conduct impact assessments and implement risk management programs. Our views are informed by our experience with members developing “Confronting Bias: BSA’s Framework to Build Trust in AI,”[2] which outlines a lifecycle-based approach for performing impact assessments to identify risks of AI bias and highlights corresponding risk mitigation best practices.

We support protecting consumers from the risks of using AI to make consequential decisions, and we are concerned several aspects of the proposed reguations are unworkable and will create significant practical challenges and unintended consequences.

We raise five concerns with the proposed regulations on ADMT:

First: The definition of automated decisionmaking technology should be clarified to help ensure the proposed regulations work in practice.

The definitions of ADMT and significant decision are critical in establishing the scope of the proposed regulations for ADMT. However, the current definitions do not create clear thresholds for identifying the technologies and decisions covered by the proposed regulations. The definition of ADMT raises three concerns:

First, automated decisionmaking technology is defined to include a broad range of software — well beyond AI systems. Unlike existing laws and proposals,[3] the definition of ADMT is not limited to AI systems. Instead, the definition of ADMT extends broadly to “technology,” including “software or programs, including those derived from machine learning, statistics, other data-processing techniques, or artificial intelligence.” As a result, the number of software tools and services that could be encompassed by the proposed regulations is staggering, as evidenced by the proposed regulations’ example of how a spreadsheet could be considered ADMT. Sweeping in such a wide range of software products and services

[2] *See* BSA | The Software Alliance, Confronting Bias: BSA’s Framework to Build Trust in AI, *available at* https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

[3] *See,* e.g., the Colorado AI Act.

creates a significant risk not just of over-regulation, but of inadvertent consequences that will arise from extending the proposed regulations well beyond their intended scope.

Second, the definition of ADMT is not aligned with the term's focus on automated technologies. ADMT is defined to include technologies that process personal information and use computation to "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." Including ADMTs that "execute a decision" creates an extremely vague and low threshold, because it's unclear what it means for an ADMT to "execute" a decision. Without further clarity, the proposed regulations could be interpreted to include ADMTs that simply carry out a decision made by a human. But the regulations should not extend to these scenarios, like using an email system to inform a housing applicant that their rental has been approved. Additionally, the definition's focus on ADMTs that "execute a decision" or "substantially facilitate human decisionmaking" detract from the term's focus on *automated* technologies, which implies technologies that make decisions with no human oversight.

Third, the definition of ADMT creates an unclear threshold for the extent to which ADMTs must influence human decisionmaking to be in scope. The proposed regulations' meaning of "substantially facilitate human decisionmaking" uses several undefined phrases, like "key factor" and "primary factor," to describe the extent to which ADMTs must influence human decisionmaking to be encompassed by the definition. Such phrases could be defined to create an objective and tailored threshold for which types of ADMTs are in scope of the proposed regulations. One way to clarify this aspect of the definition is to focus on terms such as principal basis or controlling factor; these terms have been used in other contexts and can help create a targeted threshold for the scope of the proposed regulations.

Recommendation: Section 7001(f)'s definition of ADMT should be revised to:

- Exclude "execute a decision"and "substantially facilitates human decisionmaking" from the definition of ADMT. Paragraph (f) should define ADMT as "technology that processes personal information and uses computation to replace human decisionmaking." If "substantially facilitates human decisionmaking" is retained in the definition of ADMT, we recommend clarifying "key factor" and "primary factor" to create a clear and tailored threshold for the types of decisions in scope, such as focusing on terms such as principal basis or controlling factor.
- Define covered "technologies" as AI. Paragraph 7001(f)(1) should state: "For the purposes of this definition, 'technology' means artificial intelligence."

Second: The definition of significant decision should be clarified.

The proposed regulations impose requirements when ADMTs are used "for a significant decision concerning a consumer." It is important that this term create a clear threshold, to help companies identify when these new regulations apply. We appreciate that the proposed regulations focus on decisions that result in "the provision or denial of" important benefits and services, which is a practical threshold that can help companies apply these new protections. However, the clarity of that threshold is undermined by including decisions that result in "access to" important benefits and services, a vague term that may sweep in an unintentionally broad set of activities.

Several examples illustrate the potential for confusion. For instance, a property management company may use its customer data platform to decide which contacts to email about an open house for a new apartment building. Even though the property management company is not using that platform to make decisions about whether particular individuals should be approved or denied for a specific apartment, it may be construed as using a software-based program that invites individuals to "access" housing. In healthcare, doctors offices may let their patients use websites or mobile applications to schedule appointments – thereby enabling a patient to "access" healthcare. Those scheduling functions are not the types of important life opportunities that should be the focus of the proposed regulations, but they may be unintentionally swept in by including "access" in this definition.

Further, the defintion of signifiant decision includes employment or independent contracting opportunities or compensation – and identifies three types of opportunities, including allocation or assignment of work. This part of the defintion may also sweep more broadly than intended. For example, an ADMT used to schedule shifts for hourly workers should not be subject to the same requirements as a tool that accepts or rejects an applicant from the hiring process.

Recommendation: Section 7200(a)(1) should be revised to: (1) remove "access" from the definition of "significant decision" and, (2) clarify that significant decisions are those with material, legal, or similarly significant effects on a consumer.

- The definition should state: "For the purposes of this Article, 'significant decision' means a decision that has a material, legal, or similarly significant effect on a consumer's eligibility for and results in the provision or denial of financial or lending services, housing, insurance, education or enrollment opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).
- Employment or independent contracting opportunities or compensation should not be defined to include allocation or assignment of work.

Third: The provisions on training should be reconsidered, or, at the very least, narrowed.

The proposed regulations also impose requirements for certain instances of training ADMT or AI, including obligations to: (1) conduct risk assessments (under Sections 7150(b)(4)) and 7153), (2) provide pre-use notices (under Section 7220), (3) and honor opt-out rights (under Section 7221). At the outset, the proposed regulations assume that training ADMT or AI for certain purposes is inherently problematic and should be constrained. This assumption is misguided and risks over-regulating companies' ability to train their AI systems. In actuality, thoroughly training AI systems on diverse sets of data produces more accurate and more fair outputs and can help reduce risks of algorithmic discrimination.

The proposed regulations impose requirements on businesses that use ADMT for "training uses" of ADMT, which are "processing consumers' personal information to train automated decisionmaking technology that is capable of being used for any of the following: (A) For a significant decision concerning a consumer; (B) To establish individual identity; (C) For physical or biological identification or profiling; or (D) For the generation of a deepfake." By focusing on ADMTs that *are capable* of performing certain uses, the proposed regulations will encompass a staggering range of ADMTs, a concern compounded by the broad definition of ADMT. Further, such a threshold conflates the roles of different actors along the AI value chain. For example, a company may develop an ADMT that is general in nature and could be used for hundreds, if not thousands, of different uses. Another company may then modify that general-use ADMT so that it can perform one of the specific uses encompassed by the proposed regulations. Because both companies train ADMTs that *are* *capable* of being used for one of the purposes in scope of the proposed regulations, the proposed regulations risk conflating the different roles of different companies along the AI value chain.

Further, the definition of "train automated decisionmaking technology or artificial intelligence," —which triggers the proposed regulations' obligations—creates an extremely low threshold that captures an immensely broad set of activities. Under the draft regulations, training is defined as "the process" through which an ADMT or AI "discovers underlying patterns, learns a series of actions, or is taught to generate a desired output." This encompasses many simple and mundane aspects of software development, including actions often taken by the companies that deploy AI systems, not just those that develop a broadly-used AI model. Indeed, the examples provided in this definition only exacerbate concerns regarding its breadth, as the parameters of algorithms may be adjusted hundreds, if not thousands, of times per day. Additionally, the definition of training goes well beyond a similar and broadly construed definition established by the California legislature.[4]

If the requirements on training are retained, the proposed regulations should, at a minimum, focus obligations on training ADMT — and not sweep in companies that train a range of AI systems that may present low risks. Additionally, the proposed regulations should incorporate a risk-based approach to obligations on training ADMT, to help ensure that the proposed regulations do not over-regulate companies' ability to train ADMT.

Recommendation: We strongly encourage you to reconsider the proposed regulations' requirements on training ADMT and AI and how such obligations will hamper companies' ability to thoroughly train their AI systems. If retained, Section 7001(fff)'s definition of training an ADMT or AI should be narrowed. At minimum, the proposed regulations should only focus on narrow instances of training ADMT.

Fourth: Practical implementation challenges for pre-use notices, opt-outs of ADMT, and requests to access ADMT should be addressed.

The proposed regulations require businesses to comply with sweeping obligations before using ADMT for significant decisions, extensive profiling of a consumer, or training certain uses of ADMT. These requirements present at least four concerns:

First, the proposed regulations' requirement that businesses provide consumers with pre-use notices before implementing certain uses of ADMTs will likely result in over-notification to consumers. Given the broad definitions of significant decision, training, and ADMT, the number of instances in which companies may be required to provide pre-use notices to consumers is staggering. This could result in frequent and lengthy notifications that consumers may be unlikely to read, thus undermining the protections created in the draft regulations. We strongly recommend narrowing these terms, to ensure that pre-use notices are effective in identifying processing that may create potential concerns for consumers, rather than notifying them of routine and expected processing.

Second, information required in pre-use notifications and in responses to requests to access ADMTs create several practical concerns. In some circumstances, the proposed regulations require businesses to disclose to consumers additional information in the pre-

[4] *See,* California AB 2013 (2024), which imposes transparency requirements on the data used to train generative AI systems and services. AB 2013 defines "train a generative artificial intelligence system or service" as including "testing, validating, or fine tuning by the developer of the artificial intelligence system or service."

use notifications, including the logic used in the ADMT, the key parameters that affect the output of the ADMT, and how the business plans to use the outputs of the ADMT and the role of any human involvement. Such sensitive details about the controls a business places on an ADMT and how a business uses an ADMT may include competitive or other confidential information. Since the proposed regulations do not include any protections for trade secret, intellectual property, or other confidential information, the proposed regulations may require businesses to disclose sensitive information in the pre-use notifications. Further, providing information regarding the logic behind individual consequential decisions may pose technical implementation challenges, is unduly burdensome, and will create significant impacts to companies' operations in gathering and dispersing such detailed and sensitive information.

Third, several exceptions to the proposed regulations' opt-out right rely on businesses reviewing another company's evaluation of the ADMT, which fundamentally distorts the roles and responsibilities of different types of companies and may implicate companies' trade secrets. In today's technology ecosystem, ADMTs are often developed by one company and deployed by another. Each company should be responsible for mitigating certain risks arising from the development or use of ADMTs. Such obligations, however, must be based on each company's distinct role to be workable in practice. Businesses using an ADMT will have access to information about the specific context in which an ADMT is used that is not available to the company that developed the ADMT, meaning risks specific to a particular ADMT's use may be unaccounted for if a business only relies on another company's evaluation and does not conduct its own assessment. Further, businesses may have obligations under existing state and federal laws to assess and mitigate risks of unlawful discrimination when using ADMTs in certain circumstances. Additionally, evaluating ADMTs will likely require companies to consider relevant trade secrets, intellectual property, and other confidential information in connection with the ADMT. Such information could not be reviewed by another company without creating practical and competitive concerns.

Fourth, the proposed regulations include opt-out requirements that could apply more broadly than simply allowing consumers to opt out of uses of ADMT. The proposed regulations allow consumers to opt out of certain uses of ADMT (e.g., a business does not use an ADMT with respect to the requesting consumer and instead applies a manual process), and then requires a business request that all its service providers remove a consumer from ADMT processing within a specified timeframe. Service providers' processing of opt-outs is significantly more onerous and technically challenging in the ADMT context, because ADMTs rely on a wide range of data that blends anonymized, pseudonymized, de-identified, and aggregated data about consumers. The proposed regulations should be clarified to solely require opt-outs of the uses of ADMT encompassed by the proposed regulations, which is relatively more workable and consistent with Article 11's general focus on regulating the use of ADMT with respect to consumers.

Recommendation: We encourage the CPPA to address practical concerns with requirements for pre-use notices, opt-outs of ADMT, and requests to access ADMT, including to:

- Narrow the circumstances when pre-use notices are required, by revising the definitions of significant decision, training, and ADMT.
- Clearly state that the draft regulations do not require disclosure of a business's confidential information and trade secrets.
- Adjust the opt-out exemptions to ensure they do not distort the roles and responsibilities of entities within the AI value chain.

- Clarify that consumers' requests to opt out of ADMT apply only to the uses of ADMT specified in the proposed regulations.

Fifth: The proposed regulations should be harmonized with other legislative and regulatory efforts to create clarity for businesses and consumers.

Today's technology ecosystem is global, and companies are developing strong compliance programs that can be leveraged across jurisdictions to support the responsible development and use of AI systems. As the CPPA addresses these issues, we strongly encourage you to account for the global context surrounding the draft regulations.

Even within California, legislators and other state regulators are seeking to advance proposals to regulate the use of AI tools in circumstances likely to have the most significant impact on consumers' lives. BSA is concerned that the efforts by the legislature, CPPA, and California Civil Rights Council (CCRC) risk imposing three different sets of rules on certain uses of automated tools, particularly in employment contexts — in just one state. The potential for different regulatory frameworks governing a vast range of different automated tools and services creates significant concerns and practical challenges, including for companies designing compliance programs to implement new consumer rights and protections. Unless the legislature, CPPA, and CCRC harmonize their disparate efforts to regulate the use of certain automated tools, businesses seeking to comply with their obligations will face a labyrinth of overlapping and potentially contradictory requirements and consumers will be confused regarding their rights and remedies.

Indeed, the broader context of AI regulation also counsels in favor of reading the CPPA's statutory authority to issue regulations on ADMT narrowly. Under the California Privacy Rights Act (CPRA), new regulations are to govern "access and opt-out rights with respect to business's use of automated decisionmaking technology, including profiling." This authority is phrased narrowly, to focus on the use of automated decisionmaking technology in the context of the access and opt-out rights already included in CPRA. The draft regulations appear to address issues beyond this statutory mandate, in areas where other regulators and lawmakers are actively proposing and adopting policies.

Recommendation: The CPPA should work with its counterparts in the legislature and at the CCRC to help ensure consistency in proposed frameworks governing the use of certain automated tools, which will help create clarity for businesses and consumers. The CPPA should also read its statutory mandate to issue regulations on ADMT narrowly, to decrease opportunities for potential conflicts in regulatory frameworks.

II. Cybersecurity Audits

BSA recognizes that data security is integral to protecting personal information and privacy. As the CPPA considers refinements to the proposed regulations, we encourage the agency to leverage existing standards and best practices for cybersecurity risk management, as well as established methods for demonstrating the use of practices consistent with leading security standards and frameworks.

We highlight four recommendations to integrate leading frameworks, standards, and best practices in the cybersecurity audit rules.

First: The proposed regulations should adopt a flexible, risk-based, and harmonized approach to cybersecurity auditing requirements.

Given the dynamic threat environment and risks inherent in cybersecurity, we encourage the CPPA to establish cybersecurity audit rules that are grounded in a flexible and risk-based approach, and promote consistency with existing standards, frameworks, and laws. Ensuring that the proposed regulations are harmonized with current requirements will help provide businesses with greater clarity regarding their obligations under the CCPA. This is especially important as cybersecurity regulations continue to increase internationally and at the federal and state level, each establishing new requirements and definitions that produce different approaches to compliance. Regulatory harmonization is a key goal in the White House's National Cybersecurity Strategy,[5] which encourages regulators to "harmonize not only regulations and rules, but also assessments and audits of regulated entities." Indeed, the Office of the National Cyber Director has found that "lack of harmonization and reciprocity harms cybersecurity outcomes" through increased compliance costs that draw resources away from cybersecurity programs and pose challenges to businesses of all sectors and sizes.[6]

For example, the proposed regulations would establish a set of California-specific cybersecurity auditing requirements, without referencing common frameworks, standards, and auditing criteria such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), ISO 27001, SOC 2, and programs like FedRAMP. Many organizations use these existing tools to build and maintain cybersecurity risk management programs. They are effective because they are grounded in a risk-based and flexible approach that enables organizations to tailor their risk management programs based on the needs and size of the business. In instituting an entirely new set of auditing requirements, the proposed regulations present the risk of conflicting with these existing frameworks and would establish fixed requirements that would be difficult to modify when confronted with changes in the threat environment.

Recommendation: The CPPA should adopt a flexible, risk-based, and harmonized approach to the proposed cybersecurity audit rules aligned to leading cybersecurity standards, frameworks, and laws, including the NIST CSF, ISO 27001, and the SOC 2 Type 2 audit framework.

Furthermore, Sections 7122 and 7123 of the proposed regulations outline prescriptive requirements regarding the thoroughness, independence, and scope of cybersecurity audits. As already noted, these requirements lack the flexibility that other frameworks and standards provide companies in assessing their cybersecurity programs. If the agency retains these requirements, we recommend revising them, as described below.

Recommendation:

- Modify §7122(e)(2) to state that the cybersecurity audit must: Specifically identify any *material* gaps or weaknesses in the business's cybersecurity program.

[5] The White House, National Cybersecurity Strategy (March 2023), *available at* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[6] The White House Office of the National Cyber Director, Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information (June 2024), *available at* https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

- Modify §7123(b)(2)(A)(i) to focus on phishing resistant authentication mechanisms, regardless of whether the mechanism requires single or multi-factor authentication.
- Remove §7123(b)(2)(A)(ii), regarding strong unique passwords or passphrases, as these are easily phished or stored in unsecured databases.
- Modify §7123(b)(2)(B) to state: Encryption of personal *and sensitive* information, at rest and in transit.
- Modify §7123(b)(2)(C) to state: Zero trust architecture *or least privileged access*.
- Modify §7123(b)(2)(G) to state: Internal and external vulnerability scans, penetration testing, and ~~vulnerability~~ disclosure and reporting *on patched and exploitable vulnerabilities* ~~(e.g., bug bounty and ethical hacking programs)~~.
- Modify §7123(b)(2)(H) to state: Audit-log management~~, including the centralized storage, retention, and monitoring of logs~~.
- Modify §7123(b)(2)(J), regarding antivirus and anti-malware protections to focus on endpoint detection and response (EDR) mechanisms.
- Removing §7123(b)(2)(K), as segmentation of information is primarily achieved at the network level and would be accounted for under §7123(b)(2)(I), regarding network monitoring and defenses.

Second: The proposed regulations should state that cybersecurity audits, certifications, and evaluations already performed by companies satisfy the CCPA's requirements.

One way to promote greater harmonization is to recognize that companies already perform a host of cybersecurity audits and assessments to manage cybersecurity risks. The proposed regulations should state that these audits and assessments will be accepted as compliant with the CCPA's requirements. In the United States, businesses conduct audits or assessments of their cybersecurity practices to comply with a range of federal laws including the *Sarbanes-Oxley Act (SOX)*, *Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act (GLBA), Federal Acquisition Regulation (FAR*), and *Defense Federal Acquisition Regulations Supplement (DFARS)*. In addition, the United States government requires companies supplying products or services to federal agencies to comply with FedRAMP, the U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC), and the Federal Information Processing Standards, among other requirements.

Internationally, companies often certify compliance to standards based on the Common Criteria, which underpin the Common Criteria Recognition Agreement. In Japan, the Information System Security Management and Assessment Program (ISMAP) applies cybersecurity protections to government cloud services; the United Kingdom, Korea, Singapore, and Australia have similar schemes.

In addition to existing audit requirements, customers often require their vendors to demonstrate strong cybersecurity practices — creating another layer of certifications and audit requirements. For example, customers frequently require vendors to certify they are compliant with the ISO 27000-series of standards, which govern information security management.[7] Organizations perform internal audits of information security management systems to assess their compliance with the ISO 27001 standard and prepare for external audits, which are required to obtain ISO 27001 certification. This certification can only be issued by an accredited certification body. Likewise, under the American Institute of

[7] *See* ISO/IEC 27001 and related standards, *available at* https://www.iso.org/isoiec-27001-information-security.html.

Certified Public Accountants' System and Organization Controls (SOC) framework, organizations obtain SOC 1, SOC 2, and/or SOC 3 reports and audits. The most comprehensive of these audits is SOC 2, which is an external audit performed by certified public accountants who must be independent of the organization they are assessing.

States, including California, have recognized the importance of treating companies as compliant with state requirements when they already fulfill similar federal requirements. For example, California participates in the StateRAMP program, which recognizes that companies that have invested in compliance with FedRAMP are compliant with similar obligations at the state level. The same approach is needed here.

Recommendation: Section 7123(f) should be modified to state: If the business has engaged in a cybersecurity audit, assessment, or evaluation *that is reasonably similar in scope to* ~~that meets all of~~ the requirements of this Article, the business is not required to complete a duplicative cybersecurity audit. *Illustrative examples include but are not limited to ISO 27001 certifications, SOC 2 audits, and FedRAMP authorization.* ~~However, the business must specifically explain how the cybersecurity audit, assessment, or evaluation that it has completed meets all of the requirements set forth in this Article. The business must specifically address subsections (a)–(e), including explaining how the cybersecurity audit, assessment, or evaluation addresses each component set forth in subsections (b)(1)–(2).~~ If the cybersecurity audit, assessment, or evaluation completed for the purpose of compliance with another law or regulation or for another purpose *is not reasonably similar in scope to* ~~does not meet all of~~ the requirements of this Article, the business must supplement the cybersecurity audit with any additional information required to meet all of the requirements of this Article.

Third: The proposed rules should remove the requirement that cybersecurity audits and issues raised them should be reported to the business's board of directors.

Several sections of the proposed regulations would require an auditor to report the cybersecurity audit and issues identified in the audit to the businesses' board of directors or governing body. Sections 7122(a)(2) and 7122(h) would require audits and the issues raised in them to be reported to the business's board of directors, governing body, or equivalent body.[8]

Similarly, other parts of the proposed regulations would require that the cybersecurity audit include a statement that is signed and dated by a member of the board, governing body, or if no such board or equivalent body exists, the business's highest-ranking executive who is responsible for the business's cybersecurity program.[9] Certificates of completion submitted to the agency to demonstrate that the business has performed a cybersecurity audit would also need to be signed and dated by a member of the board, governing body, or the highest-ranking executive responsible for overseeing the business's cybersecurity audit compliance.[10]

[8] California Privacy Protection Agency, California Consumer Privacy Act Regulations, Article 9. Cybersecurity Audits (§7122(a)(2) and §7122(h)) (November 2024), *available at*: https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.

[9] California Privacy Protection Agency, Cybersecurity Audit Regulations (§7122(i)).

[10] California Privacy Protection Agency, Cybersecurity Audit Regulations (§7124(c)).

We agree that boards of directors play an important role in managing a business's cybersecurity risk management, particularly by building and implementing a cybersecurity risk management strategy. However, a one-size-fits-all approach requiring reporting of cybersecurity audits directly to a business's board is not practical. While the intent behind these provisions appears to be an interest in promoting greater board accountability and oversight over a business's cybersecurity program, corporate boards already have significant visibility into the cybersecurity risks facing their organization. Businesses regularly incorporate cybersecurity risks into enterprise and cybersecurity risk management practices. Senior leaders within a business play an integral role in cybersecurity risk management by establishing the organization's risk tolerance and ensuring alignment on how to manage risk across the business. In this way, the strong cybersecurity management practices that businesses have developed allow corporate boards to support, manage, and communicate the prioritization of cyber risks.

Many companies have also started to form cybersecurity committees on their boards of directors, providing executives with more detailed insight and reporting on cyber risks. These committees promote greater communication between the board and senior leaders overseeing the business's security program, which helps ensure that cybersecurity risks are prioritized for an improved security posture.

Requiring an auditor to report cybersecurity audit issues to the board is also problematic, because board members are not themselves risk management experts and should not be expected to perform this function. Instead, the board should be able to rely on the expertise and resources of personnel with cybersecurity expertise for reporting and communication about cybersecurity risks.

Recommendations:

- Modify §7122(a)(2) to state: If a business uses an internal auditor, the auditor shall report regarding cybersecurity audit issues directly to the ~~business's board of directors or governing body, not to business management that has direct responsibility for the business's cybersecurity program. If no such board or equivalent body exists, the internal auditor shall report to the~~ business's highest-ranking executive that does not have direct responsibility for the business's cybersecurity program. *An employee*~~The business's board of directors, governing body, or highest-ranking executive~~ that does not have direct responsibility for the business's cybersecurity program shall conduct the auditor's performance evaluation and determine the auditor's compensation.
- Modify §7122(h) to state: The cybersecurity audit shall be reported to the business's ~~board of directors or governing body, or if no such board or equivalent body exists, to the~~ highest-ranking executive in the business responsible for the business's cybersecurity program.
- Modify §7122(i) to state: The cybersecurity audit must include a statement that is signed and dated by ~~a member of the board or governing body, or if no such board or equivalent body exists,~~ the business's highest-ranking executive with authority to certify on behalf of the business and who is responsible for the business's cybersecurity program.
- Modify §7123(c)(5) to state: Include the date that the cybersecurity program and any evaluations thereof were presented to the ~~business's board of directors or governing body or, if no such board or equivalent governing body exists, to the~~ highest-ranking executive of the business responsible for the business's cybersecurity program.
- Modify §7124(c) to state: The written certification must be signed and dated by ~~a member of the board or governing body, or if no such board or equivalent body exists,~~ the business's highest-ranking executive with authority to certify on behalf of the business and who is responsible for oversight of the business's cybersecurity-audit compliance.

Fourth: The CPPA should scope business's obligations and the definition of processing that presents a "significant risk" to consumers' security in line with leading cybersecurity laws, policies, and standards.

The CCPA provides that "the factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities."[11] Accordingly, the proposed regulations provide that processing is deemed to present a "significant risk" if: (1) a business derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information or (2) had annual gross revenues in excess of twenty-five million dollars and: (A) processed the personal information of 250,000 or more consumers or households in the preceding calendar year, or (B) processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.[12]

While we recognize the unique considerations involved in determining the range of businesses that will be subject to the cybersecurity audit requirement, we are concerned that the thresholds included in the proposed cybersecurity audit regulations are based on arbitrary thresholds and do not account for the fact that some companies may process personal information as both a business (for some products and services) and as a service provider (for other products and services). Because the cybersecurity audit requirements apply to businesses — and not service providers— the proposed regulations should clearly state that the cybersecurity audit requirement and its thresholds only apply to personal information that companies process in their role as businesses.

Additionally, the criteria for processing that presents a "significant risk" should be tied to high-impact risks that compromise information security, which includes risks to the confidentiality, integrity, and availability of personal information. For example, NIST has published a glossary of terms that defines "high impact" as a "loss of confidentiality, integrity, or availability [that] could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." Such a loss "might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."[13]

Appropriately scoping the definition of "significant risk" in this way would better promote a risk-based approach in the proposed regulations. Businesses have extensive experience implementing a risk-based approach to cybersecurity, and focusing on high-impact risks would further the goal of ensuring the proposed regulations are directed at the types of activities that are most likely to compromise the personal information of California's consumers.

[11] Cal. Civil Code 1798.185(a)(14)(A).

[12] California Privacy Protection Agency, Cybersecurity Audit Regulations (§7120(b)).

[13] National Institute of Standards and Technology, Computer Security Resource Center, Definition of "High Impact," *available at* https://csrc.nist.gov/glossary/term/high_impact#:~:
text=The%20loss%20of%20confidentiality%2C%20integrity,a%20severe%20degradation%20in%20mission.

Recommendation:

- Section 7120(b) should be modified to state: (b) A business's processing of consumers' personal information presents significant risk to consumers' security if *it involves a loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals and* any of the following is true:
- Modify §7123(a) to state: The cybersecurity audit must assess and document how the business's cybersecurity program protects personal information *that it processes in its role as a business* from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.

III. Risk Assessments

Data protection assessments are an important part of privacy compliance programs. BSA has supported a range of state privacy laws that require businesses to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks that may arise from those activities and to adopt appropriate mitigation measures.

We strongly recommend revising the proposed regulations to promote the use of data protection impact assessments across jurisdictions and to avoid applying California-specific documentation requirements. In many cases, businesses have already established processes for conducting and documenting privacy-related risk assessments, including under global privacy laws like the EU's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), and under state laws in 17 states.[14] We appreciate the proposed regulations' recognition in Section 7156 that when a business conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulations, it may also satisfy the obligations under CCPA. However, in practice the level of detail and content of the proposed regulations makes it impractical and highly burdensome for many companies to use assessments conducted in other jurisdictions to satisfy those obligations.

We recommend three changes to the proposed regulations' approach to risk assessments.

First: The proposed regulations should require fewer risk assessment materials be submitted to the CPPA.

Unlike leading global and state privacy laws, the proposed regulations would require businesses to proactively submit risk assessment materials to a government agency, the CPPA. This approach creates significant concerns and stands in stark contrast with leading privacy-protective approaches. None of the 17 states requiring privacy risk assessments for certain processing contain such a requirement.[15] Rather, existing laws require companies to provide risk assessments to a regulator, such as the state Attorney General, upon request if relevant to an investigation. That is the same model adopted by the EU's GDPR, which requires companies to conduct data protection impact assessments and make them available to data protection authorities upon demand. California's proposed requirement is not only at odds with other risk assessment requirements, but would also result in a

[14] *See*: BSA's 2024 Models of State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/us-2024-models-of-state-privacy-legislation.

[15] *Id*.

potentially enormous quantity of assessments flowing into the CPPA that would divert from the agency's priorities in identifying and addressing consumer harms. It would also burden California businesses without any demonstrated privacy benefits for California consumers and could compromise protected business information, such as trade secrets, as highlighted in further detail below.

Section 7157 requires businesses to submit two sets of risk assessment materials to the CPPA: (1) a certification of conduct, signed by an executive and (2) an abridged risk assessment.[16] The abridged risk assessment is to include four types of information: identification of the processing activity triggering the assessment, an explanation of the processing purposes, the categories of personal and sensitive information processed, and an explanation of the safeguards the businesses has implemented or plans to implement to address negative impacts on consumers.[17]

We strongly recommend revising this approach, to limit the types of information businesses are proactively required to disclose to the CPPA. Specifically, if businesses are required to submit materials to the CPPA proactively, those materials should be limited to certifications that the business has conducted a risk assessment. In particular, the information to be included in an abridged risk assessment under the proposed regulations can create significant privacy and security concerns. For example, if a company providing cybersecurity services discloses the categories of information it processes in order to detect cybersecurity threats, it can create a roadmap for bad actors to circumvent its security protections.[18]

These concerns are compounded because the proposed regulations do not appear to limit the CPPA's further disclosure or use of the risk assessment materials. We strongly recommend adding a provision to the proposed regulations clarifying that the CPPA will treat risk assessment materials provided to the agency as confidential and not subject to public disclosure. The proposed regulations should also specify that the disclosure of risk assessment materials to the agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.[19] This will not only help to avoid inadvertent disclosure of proprietary data and business practices that may be reflected in a risk assessment, but also help ensure strong incentives for companies to undertake rigorous risk assessments.

[16] California Privacy Protection Agency, California Consumer Privacy Act Regulations, Article 10. Risk Assessments (§7157(b)(1) and 7157(b)(2)), (November 2024), *available at*: https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.

[17] California Privacy Protection Agency, Risk Assessment Regulations (§7157(b)(2)).

[18] While section 7157(b)(2)(D), which requires businesses to explain safeguards they have adopted, recognizes that information should not be shared if it compromises a business's ability to detect and prevent security incidents, that language is not contained in other provisions of 7157(b)(2), which raise the same concerns.

[19] This protection is provided by other state privacy laws. *See, e.g.*, Colo. Rev. Stat. § 6-1-1309(4); Conn. Gen. Stat. § 42-529b(f); 6 Del. C., § 12D-108(c); Fla. Stat. § 501.713(3); Ind. Code § 24-15-6-2(b); Ky. Rev. Stat. Ann. § 367.3621(4-5); Md. Code Ann., Com. Law, § 14–4710(d)(3); Minn. Stat. § 325O.08(f); Mont. Code Ann. § 30-14-2814(3)(c-d); Neb. Rev. Stat. § 87-1116(4); N.H. Rev. Stat. Ann. § 507-H:8(III); N.J. Rev. Stat. § 56:8-166.12(b); Or. Rev. Stat. § 646A.586(7); R.I. Gen. Laws § 6-48.1-7(f); Tenn. Code Ann. § 47-18-3307(c); Tex. Bus. & Com. Code Ann. § 541.105(d); Va. Code Ann. § 59.1-580(C).

Recommendation: The CPPA should make two changes:

- First: The proposed regulations should remove Section 7157(b)(2), which requires businesses to provide the agency with an abridged version of a risk assessment. If this section is retained, only subsection (A) should be kept, and subsections (B)-(D) should be deleted.
- Second: A new provision should be added to clarify that the CPPA should classify risk assessment materials disclosed to the agency as confidential by default, exempt from open records laws, and clarify that providing the materials does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.

Second: The proposed regulations should define processing that presents a "significant risk" to consumers' privacy in line with other global and state privacy laws.

Under the CCPA, businesses must conduct a risk assessment for processing that presents a "significant risk." We strongly encourage you to adopt a definition of "significant risk" that aligns with other global and state privacy laws,[20] to support strong and interoperable compliance programs. Supporting a consistent approach in identifying the types of data for which risk assessments are appropriate also increases shared expectations about how consumers' data will be protected.

Section 7150(a) of the proposed regulations defines processing that presents a "significant risk" to consumers.[21]

In particular, we are concerned about the requirement to conduct risk assessments when personal information is processed to train automated decisionmaking technology or artificial intelligence that is *capable* of being used for: (A) a significant decision concerning a consumer; (B) to establish individual identity; (C) for physical or biological identification or profiling; (D) for generation of a deepfake; or (E) for the operation of generative models, such as large language models.[22] This language is extremely broad, particularly because it includes not just automated decisionmaking technologies but also AI broadly. This could extend the trigger for risk assessments to a wide variety of situations, including when an AI system is used in a way that was not intended by the company training the AI system.

Furthermore, the use of generative AI models, alone, is not an effective indicator of risk. Generative AI is used for a range of common low-risk uses, such as summarizing business documents and generating customer service FAQs, and therefore should not constitute the type of processing activity that would trigger risk assessment obligations. Generative AI has been widely incorporated into a variety of products of services across industry sectors, and using it as a standalone trigger for risk assessments would significantly expand the scope of products covered by this obligation, which both undermines the aim of focusing only on significant risks and substantially increases the implementation burden for companies.

[20] For example, the GDPR requires companies to conduct data protection impact assessments when processing is likely to result in a high risk to the rights and freedoms of natural persons, and 17 comprehensive state privacy laws require such assessments for specific activities presenting a heightened risk of harm to a consumer.

[21] California Privacy Protection Agency, Risk Assessment Regulations (§ 7150(a)).

[22] California Privacy Protection Agency, Risk Assessment Regulations (§7150(b)(4)).

Recommendation: The CPPA should define “significant risk” to align with other leading privacy and data protection laws, including by:

- Deleting Section 7150(b)(4), which treats training an AI system “capable” of being used in certain ways as presenting a significant risk.

Third: The proposed regulations should revise the requirements for the content to be included in risk assessments.

The content included in risk assessments should also align with content required in privacy risk assessments required under other leading privacy laws, to support strong compliance programs that work across jurisdictions.

Section 7152 sets requirements for the information to be included in a risk assessment. While some requirements align with the information organizations are required to provide in risk assessments under other global and state privacy laws, the CPPA’s proposed regulations would add new requirements that diverge from existing standards.

We are particularly concerned about Section 7152(a)(6)(B), which establishes risk assessment requirements when a business uses ADMT. Specifically, this section would require businesses that obtain ADMT from another person to identify “whether it reviewed the person’s evaluation of the automated decisionmaking technology, and whether that person’s evaluation included any requirements or limitations relevant to the business’ proposed use of the automated decisionmaking technology.”[23] This appears to assume that companies will share their risk assessments, without recognizing that assessments may contain sensitive information, including trade secrets. We strongly recommend revising this provision, to focus on how the business obtaining ADMT has evaluated that technology.

Other parts of the proposed regulations would also go beyond existing requirements for risk assessments. For example, the proposed regulations state that processing purposes cannot be identified or described in “generic terms” and would require businesses to provide information on: the minimum personal information necessary to achieve the business’s processing purpose; how long the business will retain each category of personal information; the approximate number of consumers whose personal information the business seeks to process; disclosures the business made to consumers about processing; and that a business identify whether it will initiate processing subject to the risk assessment,[24] among other new requirements. While we recognize the CPPA’s focus on potential privacy harms to California consumers, it is not clear how these requirements would enhance business’s ability to identify or mitigate risks to consumer privacy, particularly when compared to an approach that aligns with leading global and state standards.

Recommendation: The CPPA should revise the content to be included in risk assessments by:

- Modifying Section 7152(a)(6)(B)(iii)(1) to state: Where a business obtains the automated decisionmaking technology from another person, the business must identify *how it evaluated the technology*.

[23] California Privacy Protection Agency, Risk Assessment Regulations (§7152(a)(6)(B)(iii)).

[24] California Privacy Protection Agency, Risk Assessment Regulations (§7152(a)(1); (§7152(a)(2)(A); §7152(a)(3)(B); §7152(a)(3)(D); §7152(a)(3)(E); §7152(a)(7)).

- Harmonizing the content of risk assessments in Section 7152 with requirements under other state and global privacy laws.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the CPPA on these important issues.

___

For further information, please contact:

Olga Medina
Director, Policy
OlgaM@bsa.org

Meghan Pensyl
Director, Policy
meghanp@bsa.org

Business Software Alliance

From: Mark Sanchez <MSanchez@resecon.com>
Sent: Tuesday, January 14, 2025 12:15 PM
To: Regulations@CPPA
Cc: Victoria Lipnic; Paul White
Subject: Public Comment on California Consumer Privacy Act (CCPA) Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Resolution Economics Public Comments on CCPA Regulatory Updates.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Attached, please find comments from Resolution Economics, LLC.

Mark Sanchez
Resolution Economics, LLC
1155 Connecticut Ave., NW
Suite 900
Washington, D.C. 20036

resolution economics LLC

1925 Century Park East
15th Floor
Los Angeles, CA 90067

January 14, 2025

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

RE: Public Comment on California Consumer Privacy Act (CCPA) Updates, Cyber, Risk, ADMT, and Insurance Regulations

Resolution Economics, LLC, a consulting firm with offices in Los Angeles, Washington, D.C., New York, Chicago, Charlotte, and Austin, makes this submission in response to the Notice of Public Hearing and Opportunity to Comment that was issued by the California Privacy Protection Agency regarding the Proposed Regulations on the California Consumer Privacy Act ("CCPA").

We have specific experience in the area of risk assessment and evaluation of AI-enabled tools. We have been and are currently advising clients on how to evaluate the impact of and navigate compliance obligations around AI-enabled and other automated decision making and selection tools. Our experts provide independent audits that assess whether the use of AI-enabled, algorithmic, and other automated tools results in disparate outcomes with respect to race, gender, ethnicity, age, and/or other demographic categories and intersectional identities.

Resolution Economics partner Victoria A. Lipnic, head of our Human Capital Strategy Group and former Acting Chair of the U.S. Equal Employment Opportunity Commission (EEOC), led the Artificial Intelligence Technical Advisory Committee ("AI TAC") convened by the Institute for Workplace Equality. Several Resolution Economics Directors were members of the AI TAC. This multi-disciplinary group of 40 experts included labor economists, data scientists, industrial-organizational psychologists, attorneys, civil society advocates, AI vendors, employers, and former officials from the EEOC and the Department of Labor's Office of Federal Contract Compliance Programs ("OFCCP"). In December 2022, the AI TAC released the report *EEO and DEI&A Considerations in the Use of Artificial Intelligence in Employment Decision Making*. This pioneering document, one of the first to address the key issues around automatic decisionmaking technology, analyzes how professional standards, legal precedents, and principles of transparency and fairness apply to AI tools in employment decisions. It offers recommendations on data collection, employee selection procedures, statistical analysis, and addressing adverse impacts.[1]

It is our view that, when properly formulated and implemented, AI audit and assessment requirements can play a critical role in addressing the multifaceted challenges posed by artificial intelligence systems. By subjecting AI-enabled systems to rigorous evaluations and audits,

[1] https://irp.cdn-website.com/b44ff977/files/uploaded/AI-TAC%20Report%20-%20Final%20December%2021%2C%202022.pdf

potential biases and discriminatory practices can be identified. Where biases or considerable differences across demographic groups are detected in the outcome of AI-enabled systems' use, audits and assessments provide a foundation and a framework for corrective actions. The developers and/or deployers of those systems can implement appropriate remedial measures to address identified problems, enhance the fairness and inclusivity of their AI-enabled systems, and prevent future occurrences of similar issues.

Due to Resolution Economics' expertise in employment-related AI use, we have reviewed the proposed amendments to the CCPA regulations with a particular focus on the employment-related automated decisionmaking technology ("ADMT") provisions. We submit the following comments and questions regarding the Proposed Rules:

1. The current proposed regulations are unclear as to what is required for compliance

   A. What is required when evaluating ADMT systems used in employment decisions for non-discrimination safeguards?

   The proposed regulations require businesses to implement several safeguards when using ADMT for employment decisions. Businesses must conduct an evaluation of the ADMT to ensure it works as intended for the business' proposed use and does not discriminate based on protected classes (§7201). This evaluation is required when ADMT is used for significant decisions concerning employment or independent contracting opportunities or compensation or extensive profiling in employment decisions (including hiring, allocation or assignment of work and compensation, promotion, demotion, suspension, and termination). After evaluation, businesses must implement policies and procedures to ensure the ADMT works as intended and does not discriminate. Businesses must continue to provide training on these policies and procedures.

   Notably, the proposed regulations:

   - Don't specify what methods must be used for evaluation
   - Don't define standards for determining discrimination
   - Don't detail what constitutes adequate safeguards
   - Don't specify what must be included in policies, procedures, or training

   Thus, while the regulations mandate evaluation and safeguards they do not provide sufficiently clear or specific standards for compliance.[2]

[2] As a simple example regarding specific questions that may arise when evaluating an ADMT used in employment decisions, consider the issue of missing demographic information. Not all ADMTs seek data regarding race, ethnicity or gender. Even where an ADMT does ask for such information, an increasing number of individuals choose not to disclose their race, ethnicity and/or gender. The proposed regulations do not provide any guidance as to how to take into account such situations when evaluating ADMTs to ensure they work as intended for the business' proposed use and do not discriminate based upon protected classes. For instance, is imputation allowed? Should individuals who choose not to identify race, ethnicity or gender be excluded from the respective race or gender analyses?

B. Which responsibilities lie with the vendor (the provider or developer) and which lie with the user of the ADMT (the employing entity)?

The proposed regulations impose specific obligations on providers and developers of ADMTs, who must provide "all facts necessary" to businesses purchasing their systems for risk assessment purposes (§7153(a)) and must supply "plain language explanation" of system requirements and limitations (§7153(b)). Businesses using third-party ADMT must also review and validate vendor evaluations (§7152(a)(6)(B)), maintain independent safeguards regardless of vendor assurances (§7152(a)(6)(B)), and supplement inadequate vendor information (§7156(b)).

These requirements give rise to key questions, including:

- Whose responsibility is it to resolve potential disparities before and after implementation (which can potentially become much more complicated in multi-party ADMT implementations)?

- How do businesses establish a standard approach for what constitutes "adequate" vendor evaluation and independent safeguards to comply with the proposed regulations?

- What documentation and evidentiary standards will be deemed compliant to demonstrate that a business has sufficiently "reviewed and validated" a third-party ADMT's evaluation?

The proposed regulations lack specificity to provide clear guidelines differentiating vendor and user evaluation responsibilities, establish detailed protocols for managing shared responsibility scenarios, and define precise parameters for delegating monitoring duties. These gaps create significant compliance challenges for organizations seeking to implement ADMT systems while maintaining regulatory compliance.

2. The proposed regulations lack specific guidance on acceptable methodological standards for assessing ADMTs' potential discriminatory outcomes

The proposed regulations require businesses to evaluate "the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes" and "where a business obtains the automated decisionmaking technology from another person, the business must identify the following:

1. Whether it reviewed that person's evaluation of the automated decisionmaking technology, and whether that person's evaluation included any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology.
2. Any accuracy and nondiscrimination safeguards that it implemented or plans to implement" [§7152(a)(6)(B)].

The proposed regulations' ADMT evaluation requirements lack the specificity needed to answer key considerations such as:

- What specific methodological standards should be applied when identifying potential discriminatory outcomes in automated decisionmaking technology, particularly for complex machine learning systems where discrimination may not be immediately apparent?

- What specific methodological standards should be applied when businesses assess and ensure the "quality of personal information" used in ADMT systems (as required by §7152(a)(6)(B)), particularly considering that the regulations' definition of quality includes completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of sources?

- If insufficient data is available to conduct an evaluation, may synthetic/test data be used instead? If so, what features should these synthetic/test data possess?

3. <u>The proposed regulations lack clarity about who should conduct ADMT evaluations</u>

When it comes to who should review ADMT systems – and with what level of independence – the proposed regulations provide different levels of specificity for different types of assessments. They provide the most detailed standards in regard to cybersecurity audits [§7122]. For such audits, the regulations make clear that auditors may be internal or external but must exercise objective and impartial judgment, completely free from business influence. The requirements explicitly require that any cybersecurity auditor, external or internal, report directly to the board of directors, ensuring a level of organizational detachment that prevents potential biases.

The proposed regulations appear to take a different approach regarding risk assessments [§7151], primarily focusing on internal evaluation. The regulations require businesses to engage "relevant individuals" directly involved in the processing activity, typically from product, fraud-prevention, or compliance teams. No specific guidance is provided regarding how to ensure objectivity or independence in such evaluations.

The proposed regulations offer the least amount of guidance when it comes to who should conduct technology evaluations [§7201] to ensure technological performance and prevent discrimination across protected classes. This raises several key questions:

a. For internally developed ADMT, businesses must conduct their own comprehensive evaluation. The proposed regulations, however, do not address who is to perform those evaluations. Can a business use an internal or external auditor? And to whom should such auditors report?

b. When using vendor-provided technologies, the proposed regulations appear to give businesses the option to either conduct an independent assessment or review and validate the vendor's existing evaluation. However, the proposed regulations are mute about the specific methodological standards that should be applied to assess a vendor's evaluation for compliance. For example, is a vendor evaluation study acceptable if it is based on a use-case and data from another business? What about if it is based on a use-case and data from a business in a different industry?

4. The proposed regulations present significant challenges in addressing the nuanced differences between AI model types

Finally, the proposed regulations present significant challenges in addressing the nuanced differences between AI model types. While ADMT systems based on ***predictive*** AI models typically use established statistical inference methods, ***generative*** AI models create new content that requires more complex non-discrimination assessments. Hybrid AI models combining predictive and generative approaches pose the most significant evaluation challenges.

The regulations' requirement for a "plain language explanation" of ADMT logic [§7220(c)(5)] oversimplifies the complexity of modern AI architectures. From simple rule-based systems to neural networks with millions of parameters, AI models operate through intricate, often non-linear processes that resist straightforward explanation. For instance, large language models generate decisions through sophisticated interactions across interconnected nodes, where causality is probabilistic rather than deterministic. The proposed regulatory framework creates a fundamental tension between technical complexity and transparency requirements. While mandating explanation of key parameters and logic [§7220(c)(5)], the regulations do not provide concrete guidance on translating complex, high-dimensional computational processes into comprehensible terms. This approach risks forcing companies to produce explanations that are either misleadingly reductive or incomprehensibly technical.

We appreciate the opportunity to provide these comments as part of the California Privacy Protection Agency's proposed rulemaking process.

For Resolution Economics, LLC:

____
Victoria A. Lipnic, Esq.
Partner
Resolution Economics, LLC
Washington, DC

[redacted]

Paul White, Ph.D
Partner
Resolution Economics, LLC
Washington, DC

cc: Ali Saad, Ph.D., Resolution Economics, Los Angeles, CA
Margo Pave, Esq., Resolution Economics, Washington, DC
Gurkan Ay, Ph.D., Resolution Economics, Washington, DC

Grenda, Rianna@CPPA

From:	Jesse Lieberfeld <jlieberfeld@ccianet.org>
Sent:	Monday, January 13, 2025 10:53 PM
To:	Regulations@CPPA
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	CPPA Regulation Comments for submission 1-14-2025.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

January 13, 2025

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

The Computer & Communications Industry Association (CCIA) is pleased to respond to the California Privacy Protection Agency's Notice of Proposed Rulemaking on the proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations. As CPPA weighs potential modifications to the proposed Rules, CCIA offers the following proposals to guide deliberation. Attached please find our comments. Thank you for your time and consideration.

Best,

Jesse Lieberfeld
Policy Counsel
jlieberfeld@ccianet.org
O: 202-517-1536 M: [redacted]

Computer & Communications
Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.org | @CCIAnet

January 13, 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

The Computer & Communications Industry Association (CCIA)[1] is pleased to respond to the

California Privacy Protection Agency's Notice of Proposed Rulemaking on the proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations ("the proposed Rules"). CCIA supports appropriate regulation to protect both consumers and businesses. CCIA also supports greater consumer privacy protections and the goals of CCPA. However, CCIA believes that some of the draft's provisions go beyond CCPA's scope, particularly the provisions that regulate companies' back-end systems before they ever interact with consumers, and those that regulate publicly available information.

As CPPA weighs potential modifications to the proposed Rules, CCIA offers the following proposals to guide deliberation. CCIA's suggested amendments to the draft Rules are set forth in **Attachment A**.

IMPLEMENTATION

Businesses will need significant time to comply with such a large and complex set of regulations. CCIA therefore recommends that enforcement of the provisions in Articles 1, 9, 10, and 11 begin one year after the Rules' effective date.

DEFINITIONS

Section 7001(f) – "Automated Decisionmaking Technology"

This definition should be simplified considerably. It suffices to define ADMT as "any solely automated technology that processes personal information and uses computation for the primary purpose of making a solely automated significant decision about a consumer." As written, this definition conflates multiple concepts. Several points in the definition refer to "artificial intelligence" or "generative AI." Generally, automated decisionmaking includes decisions made using machine learning or AI, but not exclusively. Moreover, this definition regulates certain generative AI outputs that do not necessarily apply to consumers and would thus be outside the CCPA's scope.

[1] CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: https://www.ccianet.org/about.