
From: Hosana Brites <hosana@ujwalvelagapudi.com>
Sent: Wednesday, December 11, 2024 10:15 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: cppa_comment_ltr.docx; cppa_admt_comment_ltr.docx

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

CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Good afternoon,

Please see attached comments!

Thank you,

--

Hosana Brites

EXECUTIVE ASSISTANT TO UJWAL VELAGAPUDI
hosana@ujwalvelagapudi.com
Phone: [813-642-7895](tel:813-642-7895) (Calls and SMS only)
[+55 11 98460-5920](tel:+5511984605920) (WhatsApp only)
www.UjwalVelagapudi.com

[3 Imports LLC]

[December 10, 2024]

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

RE: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear Members of the CPPA,

I have certainly done business in California, and I've chosen not to again due to stringent regulations, etc.

For this reason, I have chosen to leave that business and the state.

Sincerely,
Ujwal Velagapudi
Business Owner
3 Imports LLC

3 Imports LLC

December 10, 2024

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

RE: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear Members of the CPPA,

I am the Business Owner of 3 Imports LLC, an on-demand Virtual Assistant platform. I no longer operate in California and don't have any clients due to stringent regulations, etc. 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 an on-demand Virtual Assistant platform that takes care of your busy work with highly vetted & trained US based assistants

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

3 Imports LLC

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 percent 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 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,
Ujwal Velagapudi
Business Owner
3 Imports LLC

From: Zane Witherspoon <[REDACTED]>
Sent: Friday, December 13, 2024 10:22 AM
To: Regulations@CPPA
Subject: Public Comment on Data Broker Price Increases
Attachments: cppa_admt_comment.docx

This Message Is From an Untrusted Sender

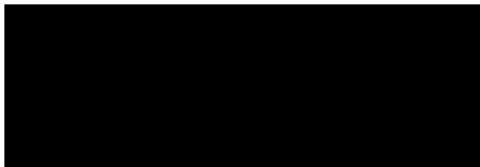
Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please see the attached comment.

--

Zane Witherspoon, CEO
Superset
The data compliance copilot



Superset Labs PBC

Dec 13, 2024

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

RE: CCPA Data Broker Registration Fee Increase

Dear Members of the CPPA,

I am the CEO of Superset Labs, an entrepreneurial venture operating in California. I am writing to express my serious concerns regarding the proposed registration price increase for Data Brokers.

Our Business and the Services We Provide

Superset exists to help small businesses navigate the complicated world of data privacy regulations across the US. We are currently helping businesses get registered as Data Brokers in California, Texas, Vermont, and Oregon.

I understand the price increase is to build out DROPS. I implore the CPPA to consider focusing on onboarding more data broker to the existing database, over building out a perfect DROPS system.

Focus on Shining the Light on Data Brokers

The DROPS program is a good initiative, but it is recreating the same technology already available in the private market many times over. I've spoken with dozens of businesses that help consumers exercise their data right to Opt-out, by *specifically reaching out to the Data Brokers in the CPPA database*

The problem consumers have with privacy isn't that there is no way to opt-out. The problem is that they don't know who has their data. If the CPPA could lower the barrier for Data Brokers to register, instead of increasing it, consumers could use the many tools already available to them to opt-out of more data sales.

The Disproportionate Impact on Small Businesses

I am deeply concerned about the disproportionate financial burden this fee places on small businesses like my customers. 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.

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

Superset Labs PBC

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. Reverse the Delete Act regulations that increase filing fees and unnecessarily expand the “data broker” and “direct relationship” definitions.
2. 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 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,

Zane Witherspoon
CEO
Superset Labs PBC

From: Mark Skvarla <mark@gpsawnings.com>
Sent: Friday, December 13, 2024 1:07 PM
To: Regulations@CPPA
Subject: More Regulations

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](#)

California Privacy Protection Agency 2101 Arena Blvd. Sacramento, CA 95834 Dear California Privacy Protection Agency Board Members and Staff, I recently learned about the decisions made by the CPPA Board at your November 8 Board Meeting and how small businesses like mine will have to handle consumer data and evaluate implementing modern technology like AI and ADMT to market or grow my business. It's concerning to small business owners like me are faced with yet another agency burdening us with new regulations and costs. Our ability to market our business, implement new and innovative technology to manage our workflow, schedule our employees and projects, oversee our inventory and shipments, and invoice our clients is essential to our growth and success. But learning that we will need to upgrade security infrastructure to meet the new standards could cost thousands of dollars—resources that I would rather reinvest into my company and employees. Moreover, the administrative load of documenting compliance and conducting regular audits pulls time and attention away from my core business activities. These requirements, while well-intentioned, risk creating an uneven playing field where only large corporations or larger businesses with dedicated legal and compliance teams can afford to compete. This is not to argue against consumer data privacy and protection. Like most business owners, I value and respect our customers' trust, and want to protect their data carefully. However, achieving compliance should not come at the expense of stifling innovation and entrepreneurship. I urge the CPPA to consider phased implementations, offering financial support or resources to help businesses adapt without undue strain. A collaborative approach between you, the regulators, and me, the business owner, is crucial for developing policies that protect consumers while enabling businesses to thrive. Thank you for the opportunity to comment on the proposed regulations.

With great hope that you can protect small business.

Mark Skvarla, CEO
GPS Specialty Construction, Inc
4240 Roseville Road
North Highlands, CA 95660
916-485-3333

From: ricoh@fairfaxlumber.com
Sent: Friday, December 13, 2024 1:27 PM
To: Regulations@CPPA
Subject: Message from "RNP583879A90C67"
Attachments: 20241213132711497.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](#)

This E-mail was sent from "RNP583879A90C67" (IM C2510).

Scan Date: 12.13.2024 13:27:11 (-0800)
Queries to: ricoh@fairfaxlumber.com

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

Dear California Privacy Protection Agency Board Members and Staff,

For more than 112 years, my employee-owned lumber and hardware store has been supplying Marin County residents with quality products and exceptional customer service. With so many agencies in California, it is hard to keep up with everything before they become a regulation I need to follow.

I recently learned that there were decisions made at your November 8 Board Meeting that represent a significant shift in how small businesses like mine will have to handle consumer data and evaluate implementing modern technology like AI and ADMT to market or grow my business. While I agree with the agency's intent to strengthen consumer privacy protections is commendable, it is essential for you to understand the burden these new regulations place on small and medium-sized businesses, like mine in Marin County.

To start, our employees are experts in lumber, hardware, and tools, not cybersecurity audits and risk assessment management. Implementing robust data governance frameworks and upgrading security infrastructure to meet the new standards could cost thousands of dollars—resources that I would rather reinvest into my company and employees.

Moreover, the administrative load of documenting compliance and conducting regular audits pulls time and attention away from my core business activities. We use automated decision-making tools to help with inventory management, set schedules, organize shipping dates and times. These requirements, while well-intentioned, risk creating an uneven playing field where only large corporations or larger businesses with dedicated legal and compliance teams can afford to compete.

I urge the CPPA to consider phased implementations, offering financial support or resources to help businesses adapt without undue strain.

A collaborative approach between you, the regulators, and me, the business owner, is crucial for developing policies that protect consumers while enabling businesses to thrive.

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

Sincerely,


Augie Venezia

Fairfax Lumber & Hardware

From: Darrell Feil <darrell@abateaweed.com>
Sent: Friday, December 13, 2024 3:17 PM
To: Regulations@CPPA
Cc: nate@kabstrat.com; Kabateck Strategies
Subject: CPPA Public Response
Attachments: CPPA_Darrell Feil_Public Comment.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

To CPPA board members,

Attached is a letter in my response to CPPA decision.

Regards,

Darrell Feil
Vice President
Abate-A-Weed, Inc.
9411 Rosedale Hwy.
Bakersfield, CA 93312
661.679.1992 office
[REDACTED] mobile
661.589.0923 fax
www.abateaweed.com

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

12/13/2024

Dear California Privacy Protection Agency Board Members and Staff,

It is apparent that the decisions made by the CPPA Board at your November 8 Board Meeting not only represent a significant shift in how small businesses like mine will have to handle consumer data, but that you have ignored the small business community in rural and central California.

It is important that you recognize the burden these new regulations place on small and medium-sized businesses and how they will impact on how we promote and market our businesses, but also how we are able to sell products and services online.

For starters, upgrading our website security infrastructure to meet your new standards could cost thousands of dollars—resources that I would rather reinvest into my company and employees. Next, the administrative load of documenting compliance and conducting regular audits pulls time and attention away from my core business activities.

These requirements, while well-intentioned, risk creating an uneven playing field where only large corporations or larger businesses with dedicated legal and compliance teams can afford to compete.

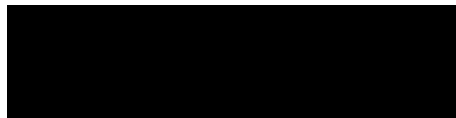
Let me be clear, this is not to say that protecting our customer data is not important and essential. What I am saying is that achieving compliance should not come at the expense of stifling innovation and entrepreneurship and disincentivizing businesses from implementing modern technologies like AI and automated decision-making tools to help run and manage our businesses.

I urge the CPPA to consider phased implementations, offering financial support or resources to help businesses adapt without undue strain.

A collaborative approach between you, the regulators, and me, the business owner, is crucial for developing policies that protect consumers while enabling businesses to thrive.

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

Sincerely,



Darrell Feil, Owner

Abate-A-Weed, Inc.

From: Ann Kinner <bridge@seabreezebooks.net>
Sent: Wednesday, December 18, 2024 12:46 PM
To: Regulations@CPPA
Subject: Proposed Regulations for AI and ADMT and Related Technology
Attachments: CPPA_Ann Kinner_Public Comment.pdf

Importance: High

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

Please see the attached and read it into the public record.

Thank you,
Ann Kinner

Seabreeze Books and Charts

1254 Scott Street, San Diego CA 92106
(619) 223-8989 bridge@seabreezebooks.net

Where in the world are YOU going?

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

December 18, 2024

Dear California Privacy Protection Agency Board Members and Staff,

I haven't been following the CPPA as closely as it appears I should have been. The decisions made by the Board at your November 8 Board Meeting represent a significant shift in how small businesses like mine will have to handle consumer data and evaluate implementing modern technology like AI and ADMT to market or grow my business.

While the agency's intent to strengthen privacy protections around consumer data is commendable, it is essential to recognize the burden these new regulations place on small and medium-sized businesses.

My small, San Diego-based, nautical book and charts store has a niche market. Our ability to promote, market, distribute, and educate current and future maritime customers on their voyages to the opening Arctic waters of the North, or throughout the islands of the South Pacific and beyond depends on my ability to use social media and contact marketing.

In recent months I've had to implement several mandated processes which have taken – and will continue to take – an inordinate amount of time to administer. The State's "one size fits all" approach simply doesn't account for a business like mine: only one part-time (10-12 hours per week) employee who supports my efforts to assist my clients and also to manage all the usual business support functions during our business hours.

Implementing robust data governance frameworks and upgrading security infrastructure to meet the new standards presented in the new regulations could cost thousands of dollars—resources that I would rather reinvest into my company and employees. Not to mention, the administrative load of documenting compliance and conducting regular audits pulls time and attention away from my core business activities.

This is not to argue against consumer privacy. Like most business owners, I value and respect our customers' trust. However, achieving compliance should not come at the expense of stifling innovation and entrepreneurship. I urge you to consider phased implementations based on both business staffing size and degree of potential exposure, offering financial support or resources to help businesses adapt without undue strain and expense.

A collaborative approach between you, the regulators, and me, the business owner, is crucial for developing policies that protect consumers while enabling businesses to thrive.

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

Sincerely,



Ann Kimmel

Seabreeze Books and Charts

Regulations@CPPA

From: Paul Cramer <paul_cramer@starmilling.com>
Sent: Wednesday, December 18, 2024 3:53 PM
To: Regulations@CPPA
Subject: Public Comment on AI and ADMT proposal
Attachments: 12.18.24 CPPA Letter.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](#)

To Whom it may concern

Attached is a letter in regards to the AI and ADMT proposed rules.

Regards,

Paul Cramer
President/COO

Star Milling Co.

www.starmilling.com

Star Milling Co.®

Member of California Grain & Feed Dealers Assn.

23901 Water Street, P.O. Box 1987, Perris, CA 92570

Phone (951) 657-3143

Fax (951) 943-2400

www.starmilling.com

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

Dear California Privacy Protection Agency Board Members and Staff,

Our family-owned business has depended on technological innovations and commitments to quality and good manufacturing processes since we started in the agriculture industry in the 1920s. Our team of all-star employees that are loyal, conscientious, and committed to our customers is what keeps us ahead of the competition. But the ability to handle logistics, market our business and wide range of feeds, and maintain our equipment depends on technologies like AI and ADMT.

The decision you made to move forward on your proposed regulations represents a significant shift in how businesses like mine will have to handle consumer data and evaluate implementing modern technology like AI and ADMT. The added burden you are putting on us with these new regulations is unfathomable.

Not only are you requiring us to implement a robust data governance framework but upgrade our digital security infrastructure to meet your new standards. This could cost thousands of dollars—resources that I would rather reinvest into my company and employees.

On top of this new added cost, the new administrative load of documenting compliance and conducting regular audits pulls time and attention away from my core business activities. I hope you understand that the risk this creates is an uneven playing field where only large corporations or larger businesses with dedicated legal and compliance teams can afford to compete.

Let me be perfectly clear, I value and respect our customers' trust, and it is essential to our business to keep their data safe and protected. However, achieving compliance should not come at the expense of stifling innovation and entrepreneurship.

I urge the CPPA to consider phased implementations, offering financial support or resources to help businesses adapt without undue strain. A collaborative approach between you, the regulators, and me, the business owner, is crucial for developing policies that protect consumers while enabling businesses to thrive.

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

Sincerely,



Paul Cramer
President/COO

Regulations@CPPA

From: joe@crispcatering.com
Sent: Thursday, December 26, 2024 11:36 AM
To: Regulations@CPPA
Subject: Costly State AI Rules
Attachments: CPPA Letter Dec 26 2024.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](#)

Good Morning

Please see the attached letter in regards to far-reaching regulations on AI

Stay Well,

Joe Thompson
Proprietor
Crisp Catering
916-600-1952 | joe@crispcatering.com
www.crispcatering.com
[X](#) | [Facebook](#) | [LinkedIn](#) | [YouTube](#)



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

December 26th, 2024

Dear California Privacy Protection Agency Board Members and Staff,

Over the last 30 years in the restaurant industry, I realize how important it is to constantly develop new ideas, keep up on the latest trends, and have exceptional customer service. Otherwise, a new restaurant will come in and overshadow you. It's the same with any small business. That is why it is essential for us to implement new technologies and ways of marketing our business, so that larger and more adaptive businesses don't push us out.

This is why the decision you made to move forward into final rulemaking on your proposed regulation at your November 8 Board Meeting was so shocking to me. This decision will cause a significant shift in how small businesses like mine will have to handle consumer data and evaluate implementing modern technology like AI and ADMT to market or grow my business. While the agency's intent to strengthen consumer privacy protections is commendable, it is essential to recognize the burden these new regulations place on small and medium-sized businesses.

For instance, implementing robust data governance frameworks and upgrading security infrastructure to meet the new standards could cost thousands of dollars—resources that I would rather reinvest into my company and employees. Moreover, the administrative load of documenting compliance and conducting regular audits pulls time and attention away from my core business activities. These requirements, while well-intentioned, risk creating an uneven playing field where only large corporations or larger businesses with dedicated legal and compliance teams can afford to compete.

This is not to argue against consumer privacy. Like most business owners, I value and respect our customers' trust. However, achieving compliance should not come at the expense of stifling innovation and entrepreneurship. I urge the CPPA to consider phased implementations, offering financial support or resources to help businesses adapt without undue strain.

A collaborative approach between you, the regulators, and me, the business owner, is crucial for developing policies that protect consumers while enabling businesses to thrive.

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

Sincerely,

Joe Thompson
Crisp Catering

From: Caitlin Seeley George <caitlin@fightforthefuture.org>

Reply-To: "caitlin@fightforthefuture.org" <caitlin@fightforthefuture.org>

Date: Monday, January 6, 2025 at 12:47 PM

To: "[REDACTED]" <[REDACTED]>

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

CPPA Chair Jennifer Urban,

I strongly urge the CPPA to adopt its proposed regulations for businesses using automated decisionmaking technologies that would protect Californians' safety, privacy, and informed consent.

These common sense rules are a vital intervention for consumer protection and human rights as unaccountable algorithms increasingly influence our housing, education, employment, and basic freedoms. These rules should reflect the needs of everyday people to be protected from discrimination and data scraping, not Big Tech's appetite for profiting from our personal info.

Please stand strong, defend our rights to algorithmic transparency and accountability, and adopt the amended regulations.

Caitlin Seeley George
caitlin@fightforthefuture.org
18625 W 59th Dr.
Golden, Colorado 80403

Regulations@CPPA

From: Ellithorpe, Katrina <Katrina.Ellithorpe@safecu.org>
Sent: Wednesday, January 8, 2025 12:29 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: SAFE CU CPPA CCPA Updates Cyber Risk ADMT and Insurance Regulations 01082025.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

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](#)

CPPA,

Thank you for the opportunity to provide comments on the proposed CCPA Updates, Cybersecurity Audits, Risk Assessments, and ADMT.

Katrina Ellithorpe (She/Her/Hers) | Senior Compliance Analyst
Direct: (916) 971-2967
safecu.org | Let us put YOU first.



This e-mail contains information from SAFE Credit Union and may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is strictly prohibited. If you have received this e-mail in error, please contact the sender immediately and delete all copies. This e-mail does not create a legally binding obligation of any kind. Any rates, terms, and conditions are subject to change. See SAFE for details.

Federally insured by NCUA | Equal Housing Opportunity



January 8, 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](#)

I am writing on behalf of SAFE Credit Union (SAFE), which serves 13 counties in Northern California. We have over 234,000 members and over \$4.6 billion in assets. SAFE respectfully submits the following comment on the proposed rulemaking to update existing California Consumer Privacy Act (CCPA) and new regulations for Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology (ADMT).

Existing CCPA Regulations

We seek clarification regarding the proposed revision to Section 7024(e), which mandates that when a request to know is denied, a detailed explanation must be provided to the consumer. This includes informing the consumer if the denial is due to a conflict with federal or state law. To ensure transparency and consistency, we would appreciate guidance on whether the business should specifically cite the relevant federal or state law, such as naming the law or regulation, referencing the U.S. Code, the Code of Federal Regulations, California law, or the California Code of Regulations. Alternatively, would a general statement indicating a conflict with federal or state law be sufficient? Providing this clarity will not only enhance the transparency of the process for consumers but also help businesses ensure compliance with the new requirements.

Cybersecurity Audits

Regarding proposed section 7122(a)(1), Thoroughness and Independence of Cybersecurity Audits, we would like to request clarification on the provision prohibiting auditors from “making recommendations” regarding the business’s cybersecurity program. While independence is critical, the wording may inadvertently restrict auditors from performing cybersecurity audits if they have previously provided recommendations based on audit findings. The auditors' role includes evaluating risks and controls and providing advisory recommendations for improvement. However, these recommendations do not constitute participation in implementation or compromise independence. We recommend revising the



SAFE

CREDIT UNION

language to clearly distinguish between providing recommendations to improve governance, risk management, or controls and participating in the implementation, design, or operation of controls. This revision would help ensure auditors can continue to offer advisory services while maintaining their independence, benefiting both businesses and consumers through enhanced cybersecurity practices.

Thank you for the opportunity to comment on the updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; and Automated Decisionmaking Technology and for considering our views.

Sincerely,

Jennifer Bradstreet
SVP, Enterprise Risk Management
SAFE Credit Union

From: Annette Bernhardt <[REDACTED]>
Sent: Thursday, January 9, 2025 6:50 PM
To: Regulations@CPPA
Cc: Annette Bernhardt
Subject: Formal Comment on Proposed Risk Assessment and ADMT Regulations
Attachments: Formal comment on proposed CCPA regulations.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

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](#)

Greetings,

Attached please find a formal comment letter from a group of 56 labor and privacy organizations and individuals.

Best,
Annette Bernhardt

Thursday January 9, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Board Members, Executive Director Soltani, and Agency Staff,

The signed organizations and individuals write to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act (CCPA). We commend Executive Director Soltani, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

For union and non-union workers alike, the emergence of AI and other data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, potentially affecting workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovations – and in particular, to ensure that workers have the ability to control the collection and use of their personal data.

A Brief Overview of Data-Driven Technologies in the Workplace

With the advent of big data and artificial intelligence, employers in a wide range of industries are increasingly capturing, buying, and analyzing worker data, electronically monitoring workers, and using algorithmic management to make important employment-related decisions.¹ Recent studies have documented the use of data-driven technologies in sectors as diverse as trucking and warehousing, hospitals and home care, retail and grocery, hotels and restaurants, call centers, building services, and the public sector. Key functions for which employers are using these technologies range from hiring and firing, to workforce scheduling, performance monitoring and evaluation, and augmentation and automation of job tasks.

While digital technologies can benefit both workers and employers, the current challenge is the lack of robust guardrails to ensure responsible use and transparency regarding which employers are using which technologies. Many legal scholars have documented the inadequacies of existing laws in the U.S. to

¹ For overviews, see Ifeoma Ajunwa, *The Quantified Worker*, Cambridge University Press (2023); Annette Bernhardt, Lisa Kresge, and Reem Suleiman, "Data and Algorithms at Work: The Case for Worker Technology Rights," UC Berkeley Labor Center (2021); Matt Scherer and Lydia X. Z. Brown, "Warning: Bossware May Be Hazardous to Your Health," Center for Democracy & Technology (2021); Wilneida Negrón, "'Little Tech' Is Coming for Low-Wage Workers: A Framework for Reclaiming and Building Worker Power," Coworker (2021); Aaron Rieke, et al., "Essential Work: Analyzing the Hiring Technologies of Large Hourly Employers," Upturn (2021); Aiha Nguyen, "The Constant Boss: Work Under Digital Surveillance," Data & Society (2021); Merve Hickok and Nestor Maslej, "A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools," AI Ethics 3, 673–687 (2023); Alexander Hertel-Fernandez, "Estimating the Prevalence of Automated Management and Surveillance Technologies at Work and their Impact on Workers' Well-Being," Washington Center for Equitable Growth (October 1, 2024).

protect workers in the data-driven workplace.² As a result of these deficiencies, direct harms to workers are beginning to emerge, with disproportionate impacts on people of color, women, and immigrants. The following examples illustrate the range in applications, impacts, and industries being documented by researchers and reported by workers:

- In warehouses, the unfettered use of productivity management systems can push the pace of work to dangerous limits and cause repetitive stress injuries for workers.³
- More generally, the COVID-19 pandemic accelerated the adoption of e-commerce throughout the retail sector. Online order fulfillment uses significant worker surveillance via the required use of phones, handheld devices, and smart glasses, as well as workplace cameras that use AI-based software to monitor worker behavior. The deployment of these technologies is not limited to fulfillment centers and workers, but extends to grocery stores and the public as well.⁴
- Bias based on race, gender, disability, and other characteristics in recruitment and hiring algorithms can mean that qualified workers are screened out from applicant pools.⁵
- Health care employers are increasingly using automated patient monitoring technology and clinical decision-making algorithms that feed into employers' algorithmic management systems to monitor nurses' work.⁶ But these systems can result in increased workloads, dangerous understaffing, heightened pressure to work faster than is safe for patients and workers, and circumventing clinical judgment of nurses and other direct care workers.⁷
- Many gig economy employers track workers and use those metrics to determine workers' access to job opportunities and to set the pay rate (which can fall below the minimum wage once expenses are factored in).⁸
- Homecare workers are increasingly required to use tablets or their phones to verify the services they've provided. But the technology—known as Electronic Visit Verification—has also been used to micromanage already very difficult care work, as well as incorporate excessive GPS monitoring.⁹
- Many low-wage employers use “just in time” scheduling software that often doesn't factor in workers' schedule constraints or prevent back-to-back or erratic assignments, wreaking havoc on workers, especially working mothers and workers of color.¹⁰

² For example, see Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, “Limitless worker surveillance,” *California Law Review*, 105(3) (2017); Brishen Rogers, *Data and Democracy at Work*, MIT Press (2023); Solon Barocas and Andrew D. Selbst, “Big Data's Disparate Impact,” 104 *California Law Review* 671 (September 30, 2016); and Pauline Kim, “Data-Driven Discrimination at Work,” *William & Mary Law Review* 58 (3): 857–936 (2017).

³ Martha Ockenfels-Martinez and Sukhdip Purewal Boparai, “The Public Health Crisis Hidden in Amazon Warehouses,” *Human Impact Partners and Warehouse Workers Resource Center* (2021).

⁴ Francoise Carre, et al. “Change and Uncertainty, Not Apocalypse: Technological Change and Store-Based Retail.” *UC Berkeley Labor Center* (2020).

⁵ Miranda Bogen and Aaron Rieke, “Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias,” *Upturn* (2018).

⁶ Peter Chan et al. “Ambient intelligence-based monitoring of staff and patient activity in the intensive care unit.” *Aust Crit Care* (Jan. 2023), 36(1): 92-98. <https://pubmed.ncbi.nlm.nih.gov/36244918/>; “National Nurses United survey finds A.I. technology degrades and undermines patient safety.” *National Nurses United* (May 15, 2024).

<https://www.nationalnursesunited.org/press/national-nurses-united-survey-finds-ai-technology-undermines-patient-safety>.

⁷ Lisa Bannon. “When AI Overrides the Nurses Caring for You.” *Wall Street Journal* (Jun. 15, 2025).

<https://www.wsj.com/articles/ai-medical-diagnosis-nurses-f881b0fe>; Bruce Giles. “I don't ever trust Epic to be correct': Nurses raise more AI concerns.” *Becker's Hospital Review* (Jun. 14, 2024).

<https://www.beckershospitalreview.com/ehrs/i-dont-ever-trust-epic-to-be-correct-nurses-raise-more-ai-concerns.html>.

⁸ Michael Reich, “Pay, Passengers, and Profits: Effects of Employee Status for California TNC Drivers,” *UC Berkeley Institute for Research on Labor and Employment*, Working Paper No. 107-20 (2020).

⁹ Alexandra Mateescu, “Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care,” *Data & Society* (2021).

¹⁰ Daniel Schneider and Kristen Harknett. “It's About Time: How Work Schedule Instability Matters for Workers, Families, and Racial Inequality,” *The Shift Project*, Harvard University (2019); Ethan Bernstein, Saravanan Kesavan, and Bradley R. Staats, “How to Manage Scheduling Software Fairly,” *Harvard Business Review* (December 2014).

But these types of negative impacts are not inevitable. We believe that employers can use data-driven technologies in the workplace in ways that benefit both workers and their businesses; the goal is not to block innovation. In fact, our organizations can offer many examples where technology has helped make jobs safer, opened up new skills and careers, and improved the quality of products and services. But it will take robust guardrails, of the kind that the CCPA begins to establish, to ensure that workers are not harmed by a rapidly evolving set of often unproven and untested technologies, many of which employers and even engineers themselves do not fully understand.

In what follows, we offer recommendations on the Agency’s proposed regulations for Risk Assessments (Article 10) and Automated Decisionmaking Technology (Article 11), building upon the policy principles that many of us shared with the Board and Agency staff in our February 26, 2024 letter. We use the term “workers” to include employees, independent contractors, and job applicants, following the CCPA’s scope in defining workplace-related personal information. Suggested deletions are in red; suggested additions are in green.

Automated Decisionmaking Technology (ADMT)

Recommendation 1: Expand the definition of Automated Decisionmaking Technology.

The data-driven transformation of the U.S. workplace is unprecedented in its speed and scope, and requires broad worker protections that respond to the range of technologies, uses, and harms. In particular, the definition of Automated Decisionmaking Technology (ADMT) will be critical to ensuring the scope of data privacy protections that the 21st Century workplace requires and that the law itself intends.

The December 2023 draft regulations defined the term ADMT to include systems that were a “whole or part of a system to make or execute a decision or facilitate human decisionmaking.”¹¹ But the final proposed regulations revise this definition to only cover systems that “execute a decision, replace human decisionmaking, or *substantially facilitate* human decisionmaking.”¹² (Italics added).

This change from “facilitates” to “substantially facilitates” creates a large opening for companies to side-step the accountability that the CPPA was charged to develop through its regulations. Essentially, an employer could self-certify itself out of coverage by the CCPA, by simply deciding that a given automated system does not “substantially facilitate” decisions by its personnel. Meanwhile, the employer could be drawing on the system to make highly consequential decisions regarding the terms and conditions of employment for its workers. But because under the proposed regulations, no one needs to be alerted that the employer is using the tool at all, neither workers nor the Agency would be able to challenge the company’s unilateral determination that the automated system’s role in a given decision-making process was not “substantial.” In our assessment, the current narrow definition of ADMT effectively creates a self-regulation regime for employers hoping to escape regulatory oversight.

¹¹ December 2023 Draft Risk Assessment Regulations, Section 7001.

¹² Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, Section 7001 (November 22, 2024).

Moreover, in practice there is significant variation in how and to what extent employers rely on automated decision-making tools.¹³ Employers may use these tools to assist them, to different degrees and in combination with many other inputs, in making critical employment-related decisions. Or, they may rely on these tools to fully automate such decisions. Harms such as discrimination, invasions of privacy, overwork injuries, and suppression of the right to organize can equally result from assistive and automated management technologies. And as several recent studies document, attempting to create fine-grained distinctions between different levels of employers' reliance on these technologies is very difficult in practice, especially given that this reliance will inevitably vary from case to case.¹⁴ In short, the full range of these use scenarios should be covered in the ADMT rights and protections being detailed in the proposed CCPA regulations.¹⁵

We therefore recommend that the Agency align with other areas of state policy and adopt the State Administrative Manual's (SAM) definition of Automated Decision System, in place of the current ADMT definition:¹⁶

Automated Decision System: A computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decisionmaking and materially impacts natural persons. An "automated decision system" does not include a spam email filter, firewall, antivirus software, identity and access management tools, calculator, database, dataset, or other compilation of data.

As an example, this SAM definition is currently being used in deliverables stemming from Governor Newsom's Executive Order on AI, such as the state's March 2024 public sector procurement guidelines.¹⁷ This definition is also increasingly being used in proposed legislation and by other regulatory agencies.

If the Agency does decide to adopt the SAM definition in its regulations, we recommend clarifying that "material impact" for the purposes of these regulations has the same meaning as the definitions of "significant decision" and "profiling."

Finally, we support other key definitions and coverage concepts in the proposed regulations regarding ADMTs. This includes the explication of "significant decisions" and "extensive profiling" in the employment context. These should not be narrowed in any future revisions to the proposed regulations.

¹³ See the studies cited in Rashida Richardson, Defining and Demystifying Automated Decision Systems, *Maryland Law Review*, 81(3):785-840 (2022) and in Maria De-Arteage, et al., "A Case for Humans-in-the-Loop: Decisions in the Presence of Erroneous Algorithmic Scores," ACM CHI '20: Proceedings of the 2020 Chicago Conference on Human Factors in Computing Systems (Apr. 21, 2020).

¹⁴ Lukas Wright, et al., "Null Compliance: NYC Local Law 144 and the Challenges of Algorithm Accountability," FAcCT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, <https://dl.acm.org/doi/10.1145/3630106.3658998> (June 2024). See also Data & Society, Comment on Proposed Rules for Implementation and Enforcement of Local Law 144 (January 23, 2023), <https://datasociety.net/wp-content/uploads/2023/01/Data-Society-AEDT-Public-comment-1.pdf>, as well as Lara Groves, et al., "Auditing Work: Exploring the New York City Algorithmic Bias Audit Regime," FAcCT '24 (June 2024), <https://facctconference.org/static/papers24/facct24-74.pdf>.

¹⁵ See Grace Gedy and Matt Scherer, "Are These States About to Make a Big Mistake on AI?," Politico (April 30, 2024).

¹⁶ California Department of General Services, State Administrative Manual, Definitions - 4819.2 (last revised March 2024). Accessed at <https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2>.

¹⁷ California Department of Technology, "State of California GenAI Guidelines for Public Sector Procurement, Uses and Training" (March 2024). Accessed at <https://www.govops.ca.gov/wp-content/uploads/sites/11/2024/03/3.a-GenAI-Guidelines.pdf>.

Recommendation 2: Strengthen notice and access rights for workers when an employer has used an ADMT to make a decision about them.

One of the hallmarks of the CCPA is that it recognizes the importance of transparency and disclosure in order for consumers and workers to make informed decisions about their data privacy. But currently, the biggest obstacle to ensuring responsible use of data-driven technologies in the workplace is that they are largely hidden from both policymakers and workers. Without transparency and disclosure, job applicants won't know why a hiring algorithm rejected their resume; truck drivers won't know when and where they are being tracked by GPS; and workers won't realize their health plan data is being sold. In an especially pernicious example, some employers are using surveillance to identify workers who are trying to organize a union, as well as predictive algorithms that data-mine social media to identify workers who might be *likely* to try to organize one.¹⁸

Given the “black box” nature of much of digital workplace technology, notice and access rights will be critical for California’s workers, who need to know what types of ADMTs are being used to make critical decisions about them, including which traits or attributes the ADMTs analyze and the methods by which they measure those traits or attributes. This information is particularly important for ADMTs that require the worker to input information or otherwise interact with the ADMT, since such information is needed to ensure that workers entitled to accommodation under applicable law, such as workers with disabilities, know whether they need to request accommodation.

Equally important, once such a system has been used to make an employment-related decision, workers should have the right to know what model was used, what the inputs were, and crucially, what the outputs were and how the employer used them. Such disclosures are the first step in workers’ ability to identify and challenge errors and unfair treatment. To illustrate, consumer-facing industries are increasingly incorporating customer ratings in their worker assessment systems. But we know that customer ratings are highly unreliable and carry significant risk of bias and discrimination on the basis of race, gender, accent, and other characteristics.¹⁹ Without disclosure that these ratings have been used to evaluate them, and how, workers are left in the dark about the actual determinants of their performance evaluations.

Importantly, we do not believe that these notice requirements will be onerous on employers. For pre-use notice, the required information consists of information that companies will already have in their possession. For hiring algorithms, the notice can be given at the time of application; for incumbent workers, the notices can be automated and given to workers as part of the onboarding process and annually thereafter to remind workers of the systems in use. Similarly, notice of actual use of such systems, and workers’ right to access more information about that use, can be routinized and automated, and is in line with general notice requirements already established by the CCPA.

We support the overall structure and substance of the notice and access rights; these should not be weakened in any future revisions of the regulations. That said, we recommend the following three changes to ensure that these provisions are sufficiently strong to protect workers in the use of ADMTs.

¹⁸ Susan Berfield, “How Walmart Keeps an Eye on Its Massive Workforce: The Retail Giant Is Always Watching,” Bloomberg BusinessWeek (November 24, 2015). For more on the importance of transparency, see also the recent guidance by the Consumer Finance Protection Bureau, “Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions,” Consumer Financial Protection Circular 2024-06 (October 24, 2024).

¹⁹ Alex Rosenblat, Solon Barocas, Karen Levy, and Tim Hwang, “Discriminating Tastes: Customer Ratings as Vehicles for Bias,” Data & Society (2016).

Recommendation 2.1: Expand the definition of an “adverse significant decision” triggering additional access notice requirements. The proposed regulations rightly identify key adverse decisions in the employment context, such as termination and loss of compensation. Two other types of adverse decisions should be included in this list, since they have significant impacts on workers: disciplinary actions (such as being put on probation, not being promoted, and being transferred involuntarily) and changes to working hours and shifts (which are common and can wreak havoc on the lives of low-wage women workers in particular). We recommend the following changes:

Section 7222(k)(1)(A): Resulted in a consumer who was acting in their capacity as a student, employee, or independent contractor being denied an educational credential; having their compensation decreased; ~~or~~; being suspended, demoted, terminated, disciplined, or expelled; having changes to work hours and shift assignments; or

Recommendation 2.2: Reinstate the requirement that allows a worker to access aggregate outputs relevant to the use of an ADMT with respect to the worker. A key component of transparency and disclosure of ADMT use in the workplace setting is providing aggregate comparison data so that workers can understand the context in which their own data was analyzed. We therefore recommend the following changes to Section 7222(b)(4):

(4) How the automated decisionmaking technology worked with respect to the consumer. At a minimum, this explanation must include subsections (A), ~~and~~ (B) and (C):

(A) How the logic, including its assumptions and limitations, was applied to the consumer; ~~and~~

(B) The key parameters that affected the output of the automated decisionmaking technology with respect to the consumer, and how those parameters applied to the consumer.

(C) ~~A business also may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers. For example, a business may provide the five most common outputs of the automated decisionmaking technology, and the percentage of consumers that received each of those outputs during the preceding calendar year.~~ A simple and easy-to-use method by which the consumer can obtain the range of possible outputs, which may include aggregate output statistics (for example, the five most common outputs of the automated decisionmaking technology, on average, across all consumers during the preceding calendar year, and the percentage of consumers that received each output during the preceding calendar year).

Recommendation 2.3: Clarify that a worker has the right to use an authorized representative to access information relevant to the use of an ADMT with respect to the worker. The ability of workers to exercise their rights under the CCPA will depend crucially on their ability to designate representatives to act on their behalf, including unions and other worker organizations, since research has shown that accessing data rights can be challenging to navigate, especially for individuals who may lack the resources or expertise.²⁰ We therefore recommend the following provision be added to Section 7222.

²⁰ Jef Ausloos and Pierre Dewitte, “Shattering One-Way Mirrors – Data Subject Access Rights in Practice.” International Data Privacy Law 8, no. 1 (February 1, 2018).

A consumer may use an authorized agent to submit a request to access information about a business's use of an automated decisionmaking technology on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

Recommendation 3: Restore a meaningful right for workers and consumers to opt-out of consequential ADMT systems.

A key hallmark of the CCPA is that it establishes a baseline level of agency for consumers and workers, such as the right to correct their data or to opt-out of the sale or sharing of their data. The proposed CCPA regulations detail several additional touchpoints for personal agency that will be especially important to workers. In particular, workers should have the right to opt-out of harmful, consequential, or especially intrusive automated decision-making systems, just as consumers do. There are important policy precedents for this approach.

For example, a range of public policies and collective bargaining agreements in the U.S. and other countries recognize the importance of allowing workers to refuse to work in conditions that are harmful to their physical or mental health.²¹ In leading privacy policy models, highly consequential decisions require human review and can not be automated; an example in the workplace context is that workers should be able to opt-out of or challenge the use of automated hiring and firing systems, given their significant economic impact.²² Similarly, workers should have the right to preserve their privacy against highly intrusive monitoring systems by opting out of them. For example, the ubiquity of electronic monitoring and data collection systems have increased the ability of employers to monitor workers off-duty, including social media eavesdropping.²³ And in the retail industry, vendors have developed software that mines data from workers' social media accounts to predict whether a job candidate will become a whistleblower.²⁴

Unfortunately, the proposed regulations effectively eliminate the ability for workers to protect themselves by opting-out of consequential ADMT systems. The December 2023 draft regulations provided consumers with opt-out rights for uses of ADMTs to make decisions that produce "legal or similarly significant effects."²⁵ The revised draft adds a complex series of exceptions to those opt-out rights specifically for workers, and more generally for consumers, and the impact will be to undermine their agency over how they are tracked, profiled, evaluated, and potentially harmed by algorithmic tools.

²¹ For examples of policies and collective bargaining provisions establishing workers' right to refuse unsafe work, see "Collective Bargaining Language - Health and Safety Rights," Labor Occupational Health Program, University of California, Berkeley (2024). For an overview of the negative mental health impacts of electronic monitoring, see Lisa Kresge and MT Snyder, "35 Years Under Electronic Monitoring and Still Waiting for Worker Rights," UC Berkeley Labor Center (2023).

²² Many AI principles frameworks, including the White House's Blueprint for an AI Bill of Rights, include some version of the right to opt-out of automatic decision-making systems that pose significant risks or harms, especially in sensitive domains including employment. For example, Article 22 of the GDPR establishes an individual's right not to be subject to a consequential decision based solely on automated data processing.

²³ Richard Bales and Katherine Stone, "The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace," Berkeley Journal of Employment & Labor Law 41 (1) (2020).

²⁴ See for example, <https://fama.io/retail-hospitality/>.

²⁵ See December 2023 Draft Risk Assessment Regulations, Section 7030.

Ultimately, legislation will be needed to fully protect the rights of workers and consumers in California in the use of ADMTs. In the meantime, our recommendations in this section are intended to restore a meaningful right for workers and consumers to opt-out of consequential ADMT systems, consistent with the language and purpose of the CCPA.

Recommendation 3.1: Add guardrails on the “security, fraud prevention, and safety exception” to prevent businesses from misusing it. Businesses can readily misclassify or misuse the results of ADMTs as evidence of “fraud” or “dishonesty,” harming California consumers and workers.²⁶ First, we recommend the business must show that its use of ADMT under this exception is both “strictly necessary” and “proportionate.” Both are well-established principles under the GDPR.²⁷ Second, consumers must have a right to a written explanation for why the ADMT is strictly necessary and proportionate so they can act as whistleblowers in case of a business’s misuse of this exception. Third, in the case of allegations for fraud or dishonesty, businesses should be required to make their allegations with specificity—a long-standing legal principle to deter non-meritorious fraud allegations and to ensure that the party charged with fraud can intelligently respond to the allegations.²⁸ This is particularly important in the ADMT context, in which workers are likely to be at a heightened informational disadvantage in comparison to the business that made the ADMT decision.²⁹ Specifically, we recommend that Section 7221 (b)(1) be revised as follows:

- (1) If all of the following are true: (“security, fraud prevention, and safety exception”)
 - (A) The business’s use of that automated decisionmaking technology is proportionate and strictly necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below:
 - (i) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;
 - (ii) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or
 - (iii) To ensure the physical safety of natural persons.
 - (B) The consumer has a right to request to obtain, pursuant to the procedures in Section 7222, a sufficiently precise and adequately substantiated explanation of why the business’s use of automated decisionmaking technology is strictly necessary and proportionate to accomplish the allowable purpose as specified in Section 7221(b)(1)(A).
 - (C) For any decision concerning a consumer as set forth in Section 7221(b)(1) that involves allegations of fraud or dishonesty by the consumer, the business must provide, in writing, specific details on any allegations of fraud or dishonesty and provide the consumer with an opportunity to appeal such allegations.

²⁶ For example, in the context of online labor platforms, a business’s failure to correctly recognize a worker using facial recognition software can be characterized by the business as fraudulent use of the platform, which can lead to the worker’s suspension or termination. See, e.g., “[Uber’s Anti-Fraud Systems](#) and the Failure of Human Review,” Worker Info Exchange, May 14, 2021; “[Road to Nowhere](#),” Chicago Gig Alliance and the People’s Lobby, 2023, p. 5.

²⁷ See, e.g., GDPR, [Recital 47](#) and [European Data Protection Supervisor](#).

²⁸ See, e.g., *Committee on Children’s Television v. General Foods Corp.* (1983) 35 Cal.3d 197, 216–217 (“*Committee on Children’s Television*”).

²⁹ Sara Baiocco, Enrique Fernández-Macías, Uma Rani and Annarosa Pesole, “The Algorithmic Management of Work and its Implications in Different Contexts,” JRC Working Papers Series on Labour, Education and Technology 2022/02, p. 22 (noting the information asymmetries and power imbalances that arise between management and workers in the context of algorithmic management).

Recommendation 3.2: Eliminate the overly broad “hiring,” “allocation/assignment of work and compensation,” and “work profiling” exceptions under Sections 7221(b)(3), (b)(4), and (b)(5). These exceptions only require a company to assert that the ADMT in question is “necessary” to achieve some purpose, and to evaluate in some undefined way the ADMT for accuracy and non-discrimination (the latter is no added protection at all, since these anti-discrimination protections are already provided for under Sections 7152(a)(5) and 7152(a)(6) in the proposed regulations.³⁰ Such vague and broad categorical exceptions threaten to deprive workers of agency over algorithmic tools that can have significant impacts on their work and livelihoods, as well as their right to protect their personal data.

Recommendation 3.3: Strengthen the human review and appeal requirements under the “human appeal exception.” We recommend significant strengthening of the human appeal exception, on three fronts. First, by only requiring that the human reviewer be “qualified” and “have the authority to overturn the decision,” the proposed regulations insufficiently mitigate the risks of partiality and of human reviewers excessively deferring to algorithmic decisionmaking, given that the same business will be both making and evaluating the appeal of the ADMT decision. We therefore recommend two requirements derived from the European Union Platform Directive: (1) mandating that the business allocate sufficient human resources to ensure effective appeals for the decision, and (2) expressly protecting human reviewers from retaliation for overturning ADMT decisions.³¹ We also recommend training, impartiality, anti-bias, and conflict of interest-related protections. These protections are derived from Title IX, which can serve as a comparable regulatory framework that significantly relies on internal dispute resolution systems.³²

Second, the proposed regulations make it unnecessarily onerous for consumers to pursue an appeal. Given that many consumers will face significant barriers in the ADMT appeal process—language, disability, literacy, etc.—the proposed regulations should expressly authorize that a business must permit the consumer to be represented by an authorized agent or advisor of their choice.³³ We also identify several additional procedural protections to deter arbitrary decisionmaking by the business.³⁴

Third, in the event that a human reviewer finds that a covered ADMT decision has infringed upon the rights of a consumer, we recommend that the business be required to undertake certain actions to deter and prevent such erroneous decisions in the future. This recommendation is modeled on the European Platform Directive.³⁵

Specifically, we recommend that Section 7221(b)(2) be revised as follows:

- (2) For any significant decision concerning a consumer as set forth in Section 7200, subsection (a)(1), if the business provides the consumer with a method to appeal the decision to a qualified human reviewer who is required to objectively evaluate all relevant evidence and has the authority to overturn the decision (“human appeal exception”). To qualify for the human appeal exception, the business must do the following:
 - (A) The business must designate a human reviewer who:

³⁰ Specifically, Section 7152(a)(5)(B) requires the business, as part of its mandated risk assessment, to identify “[d]iscrimination upon the basis of protected classes that would violate federal or state antidiscrimination law.” Section 7152(a)(6) requires the business to identify the safeguards that it plans to implement to address discrimination and other potential negative impacts.

³¹ E.U. [Platform Directive](#), Article 10.2.

³² See, e.g., 34 C.F.R. § 106.45(d)(3)(iii)-(iv); 34 C.F.R. § 106.8(d)(2).

³³ See, e.g., 34 C.F.R. § 106.46(c)(1)(ii).

³⁴ 34 C.F.R. § 106.45(h)(2); see also [E.U. Platform Directive](#), Art. 11.1, 11.2.

³⁵ E.U. [Platform Directive](#), Article 11.3.

- (i) Is trained and qualified to understand the significant decision being appealed, ~~and~~ the consequences of the decision for the consumer, how to evaluate the decision, and how to serve impartially, including by avoiding prejudgment of the facts at issue, conflict of interest, and bias;
 - (ii) Does not have a conflict of interest or bias for or against the business or the consumer generally, or against the business or consumer specifically;
 - (iii) Was not involved in the initial decision being appealed;
 - (iv) Must enjoy protection from dismissal or its equivalent, disciplinary measures, or other adverse treatment for exercising their functions under this section; and
 - (v) Must be allocated sufficient human resources by the business to conduct an effective appeal of the decision.
- (B) This human reviewer must consider the relevant information provided by the consumer in their appeal and may consider any other sources of information about the significant decision.
- (C) The business must clearly describe to the worker how to submit an appeal and enable the worker to submit corrections or otherwise provide information, evidence, and a written statement in support of or challenging the outcome, for the human reviewer to consider as part of the appeal.
- (i) The method of the appeal must also be easy for the workers to execute, require minimal steps, and comply with sections 7004 and 7020.³⁶
 - (ii) The business must permit the worker to be represented by an authorized agent or advisor of their choice, who may be, but is not required to be an attorney.
 - (iii) In responding to the appeal, the business must provide the consumer with a sufficiently precise and adequately substantiated reply in the form of a written document, describing the result and explaining the reasons for its decision, which may be in electronic format.
 - (iv) In the event that the significant decision in paragraph (b)(2) of this section is found by the human reviewer to have infringed on the rights of the consumer, the business shall rectify that decision without delay and in any case within fourteen calendar days of the finding by the human reviewer. The business shall also take the necessary steps in order to avoid such decisions in the future, including, if appropriate, a modification of the ADMT or a discontinuance of its use.

Recommendation 3.4: Require ex-ante human review and expedited appeals for “highly-consequential decisions” when claiming the human appeal exception. A majority of Americans consistently report that they are uncomfortable with the use of artificial intelligence in high-stakes decisions about their lives.³⁷ Especially when it comes to consequential decisions like the loss of one’s job, workers should have a right to human review *before* an ADMT-assisted decision takes place – not afterwards, when a harm may already have occurred. Research indicates that when using an automated system, people are biased towards accepting the outcomes the system produces even when other factors indicate that the results

³⁶ Consistent with this reference to Section 7020, we also recommend that Section 7020 be revised so that the same methods which currently apply to the submission of requests to know, delete and correct also apply to the submission of requests to appeal ADMT.

³⁷ Consumer Reports, [Survey](#), Jul. 25, 2024.

are wrong, undermining the protections of a human appeal process.³⁸ In light of these risks, we recommend a stronger set of requirements for businesses who wish to claim the human appeal exception when using ADMTs to make highly-consequential decisions about their workers. In these cases, human review should be required before the decision is made.

Specifically, we recommend that the following new Section 7221(b)(2)(D) be added for “highly-consequential decisions”:

- (D) For uses of ADMTs in making hiring, firing, disciplinary, or compensation-related decisions as set forth in Section 7200(a)(1)(B)(i)-(iv) (“highly consequential decisions”), the business must in addition do the following in order to claim the “human appeal exception”:
- (i) The business must conduct its own evaluation of the consumer before making the highly consequential decision, independent of the output used from the ADMT.
 - (ii) This includes establishing meaningful human oversight by a designated internal reviewer to corroborate the ADMT output by other means. Meaningful human oversight requires that the designated internal reviewer meet the following conditions:
 - 1. The designated internal reviewer is granted sufficient authority, discretion, resources, and time to corroborate the ADMT output;
 - 2. The designated internal reviewer has sufficient expertise in the operation of similar systems, and a sufficient understanding of the ADMT in question to interpret its outputs as well as results of relevant risk assessments; and
 - 3. The designated internal reviewer has education, training or experience sufficient to allow the reviewer to make a well-informed decision.
 - (iii) Where a business cannot corroborate the ADMT output produced by the ADMT, the business is prohibited from relying on the ADMT to make the highly-consequential decision.
 - (iv) When a business can corroborate the ADMT output and makes the highly-consequential decision, the business must notify the consumer of the consumer’s right to appeal, as described in proposed Section 7221(b)(2)(C) above. All information and judgments involved in the business’s corroboration of the ADMT output must be communicated to the consumer as part of this appeal notification, and the business must follow the appeal response timelines for highly consequential decisions set forth in Section 7021(b).

Recommendation 3.5: Shorten the appeal timelines for the “highly consequential ADMT decisions” (as defined in Recommendation 3.4). The proposed regulations currently allow a business between 45 and 90 days to process an appeal of an ADMT decision. Considering that more than half of Americans live paycheck to paycheck, this timeline could result in significant economic harm in the context of a highly consequential ADMT decision like a firing, suspension, or demotion.³⁹ We recommend a two-week deadline for a business to respond to a consumer’s appeal of a highly consequential ADMT decision. This

³⁸ This bias can make human oversight ineffective at curbing the worst harms of ADMT, as the human meant to act as a final judge will often take the system’s output as preferable to their analyses, even disregarding evidence to the contrary. Mary L. Cummings, *Automation and Accountability in Decision Support System Interface Design*, 32 J. Tech. Stud. 23, 25 (2006). See also Saar Alon-Barkat and Madalina Busuioc, *Human–AI Interactions in Public Sector Decision Making: “Automation Bias” and “Selective Adherence” to Algorithmic Advice*, 33 J. Pub. Admin. Rsch. and Theory 153, 155 (2022) (“Automation bias refers to undue deference to automated systems by human actors that disregard contradictory information from other sources”), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794660.

³⁹ United States Interagency Council on Homelessness. “Data and Trends.” <https://www.usich.gov/guidance-reports-data/data-trends>.

is modeled on the European Union’s Platform Directive.⁴⁰ Specifically, we recommend that Section 7021(b) be revised as follows:

- (b) Businesses shall respond to a request to appeal a highly consequential ADMT under Section 7221(B)(2)(D) no later than 14 calendar days after receipt of the request. For all other requests, bBusinesses shall respond to a request to delete, request to correct, and request to know, request to access ADMT, and request to appeal ADMT no later than 45 calendar days after receipt of the request . . . [same]

Recommendation 3.6: Expressly prohibit businesses from retaliating against consumers who have exercised their access and appeal rights. Retaliation by businesses on such opt-out grounds is clearly prohibited under Civil Code Section 1798.125, subdivisions (a)-(b).⁴¹ This recommendation is consistent with the rationale provided in the October 2024 Draft Initial Statement of Reasons, which states that the addition of subdivision (l) is to “facilitate[] compliance with the [CCPA’s] statutory prohibition against retaliation . . . [by] consolidat[ing] the relevant requirements for the right to opt-out of ADMT in one place.”⁴² Specifically, we recommend that Section 7221(l) be revised as follows:

- (l) A business must not retaliate against a consumer because the consumer exercised their opt-out right, including, but not limited to, their right to opt-out of the use of an ADMT, their right to access details about an ADMT-assisted decision, or their right to appeal an ADMT-assisted decision, as set forth in Civil Code Section 1798.125 and Article 7 of these regulations.

Risk Assessments

The proposed regulations detail an important set of procedures for providing notice of risk assessments of data collection and automated decision-making systems. Such assessments are widely considered a critical tool for identifying and mitigating harmful impacts of digital technologies.⁴³ In the workplace context, conducting risk assessments prior to use will be absolutely critical; it is not fair to workers to wait until invasions of privacy and other harms have already occurred to begin regulatory oversight. Moreover, conducting risk assessments prior to use also helps to identify potential design flaws and harms early on, when they are easier and less costly for developers and employers to address.⁴⁴ Here too we do not believe these requirements to be onerous for employers, because the proposed regulations include an exemption for routine administrative data processing.

Recommendation 4: Strengthen the required elements of risk assessments.

The proposed regulations deliver a critical framework for ensuring that businesses consider the risks posed to consumers and workers by the use of automated decisionmaking technology. The regulations

⁴⁰ [E.U. Platform Directive](#), 11.1, 11.2.

⁴¹ These subdivisions broadly prohibit businesses from discriminating or retaliating against a consumer “because the consumer exercised any of the consumer’s rights under this title.” Cal. Civ. Code § 1798.125, subd. (a)(1).

⁴² “[Draft Initial Statement of Reasons](#),” California Privacy Protection Agency, Oct. 4, 2024, p. 91.

⁴³ Emanuel Moss, et al., “Assembling Accountability: Algorithmic Impact Assessment for the Public Interest,” *Data & Society* (2021); Daniel J. Solove, “Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data,” *Northwestern University Law Review* 118 (2024).

⁴⁴ Henriette Cramer, et al., “Assessing and Addressing Algorithmic Bias in Practice,” *Interactions* 25, no. 6 (October 25, 2018); Andrew Selbst, “An Institutional View of Algorithmic Impact Assessments,” *Harvard Journal of Law & Technology* 35, no. 1 (2021).

contain key elements to making risk assessments a meaningful part of protecting the privacy and rights of working people. In order to ensure that the proposed regulations clearly communicate safeguards put in place by businesses, the reported purposes of ADMTs, and the categories of harms that could still impact people in the workplace, there are several sections that could be enhanced. To ensure greater transparency and accountability to workers, we recommend reinstating several elements of the December 2023 draft of the regulations outlined below.

Recommendation 4.1: Explicate the worker harms that risk assessments must test for. It is important to understand that while automated hiring systems have captured the most attention in public debate, they are only the tip of the iceberg. Employers' use of data-driven technologies happens throughout the entire employment lifecycle – and negative effects on privacy, race and gender equity, and other important aspects of employment can result throughout. Important employment-related decisions include hiring and recruitment; setting of wages, benefits, hours, and work schedules; performance evaluation, promotion, discipline, and termination; job assignments, productivity requirements, and workplace health and safety; decisions that result in job augmentation, automation, and access to upskilling opportunities; and other terms or conditions of employment. In order to ensure that the proposed regulations clearly communicate how the existing categories of harms might manifest in the workplace, we recommend the following edits to Section 7152(a)(5):

(D) Coercing or compelling consumers into allowing the processing of their personal information, such as by conditioning consumers' acquisition or use of an online service upon their disclosure of personal information that is unnecessary to the expected functionality of the service, or requiring consumers to consent to processing when such consent cannot be freely given, for example as a condition of employment.

(F) Economic harms, including but not limited to limiting or depriving consumers of economic opportunities via firing, discipline, or denial of promotion, reducing compensation, task or job automation, or reclassification of workers' employment status; charging consumers higher prices; compensating consumers at lower rates; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.

(G) Physical harms, to consumers or to property, including processing that creates the opportunity for physical or sexual violence, or physical harms stemming from productivity management systems that speed up the rate of work to the point of injury.

(I) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation. Psychological harm includes, for example, emotional distress resulting from disclosure of non consensual intimate imagery; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; stress resulting from pervasive surveillance at work or automated productivity quotas; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

We also recommend reinstating the following provision from the December 2023 draft regulations:

Constitutional harms, such as chilling or deterring consumers' free speech or expression, political participation, religious activity, free association, freedom of belief, freedom to explore ideas, or reproductive freedom; and harms to consumers' ability to engage in collective action or that impede the right to unionize.

Recommendation 4.2: Strengthen the safeguards against harmful ADMTs that businesses are required to disclose. As the proposed regulations already identify in Section 7152(a)(5), the potential negative impacts associated with the processing of personal information include discrimination, but also a range of other potential harms. Section 7152 (a)(6)(B) in the proposed regulations should therefore pertain to all of the harms identified in risk assessments, rather than only discrimination based on protected classes. We recommend these additions to Section 7152 (a)(6)(B):

(B) For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3), the business must identify the following:

(i) Whether it evaluated the automated decisionmaking technology to ensure it works as intended for the business’s proposed use and does not discriminate based upon protected classes or contribute to other negative impacts to consumers’ privacy set forth in Section 7152(a)(5) (“evaluation of the automated decisionmaking technology”); and

(ii) The policies, procedures, and training the business has implemented or plans to implement to ensure that the automated decisionmaking technology works as intended for the business’s proposed use and does not discriminate based upon protected classes or contribute to other negative impacts to consumers’ privacy set forth in Section 7152(a)(5) (“accuracy and nondiscrimination safeguards”).

We also recommend the following addition to Section 7152(a)(6), to ensure that workers and consumers have a better understanding of the risks that may impact them:

The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5). The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; whether there are any residual risks remaining to consumers’ privacy after these safeguards are implemented and what these residual risks are; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures.

Recommendation 4.3: Require businesses to be more clear about the purpose of ADMTs. Section 7152(a)(1) in the proposed regulations states: “The business must specifically identify its purpose for processing consumers’ personal information.” We recommend strengthening this disclosure by reinstating several clarifications present in the December 2023 draft regulations, as follows:

The business must specifically identify its purpose for processing consumers’ personal information, how the processing achieves that purpose, and the purpose’s compatibility with the context in which the personal information was collected. The purpose must not be identified or described in generic terms, such as “to improve our services” or for “security purposes.”

Recommendation 4.4: Strengthen the required disclosure of risk assessments by increasing transparency around the lack of external party consultation. Reinstating provision Section 7151(b)(1) from the December 2023 draft of the regulations would ensure that businesses explain why they chose not to engage external stakeholders. We recommend reinstating this provision:

For the uses of automated decisionmaking technology or artificial intelligence set forth in Section 7150, subsections (b)(3) and (b)(4), if the business has not consulted external parties in

its preparation or review of the risk assessment, the risk assessment shall include a plain language explanation addressing why the business did not do so and which safeguards it has implemented to address risks to consumers' privacy that may arise from the lack of external party consultation.

Recommendation 5: Clarify the role of workers and unions in risk assessments.

There is growing consensus among technology researchers that workers are important stakeholders that should be involved when their employers conduct risk assessments, whether of data collection systems or of automated decision-making systems.⁴⁵ That is both a matter of principle, but also a matter of good practice. Workers have a significant amount of firm-specific knowledge and experience to bring to the table; their input can be vital for assessing and implementing new technologies.⁴⁶

A good example of the importance of worker involvement comes from new technologies in the hotel industry that automate housekeeper tasks and can result in inefficient orderings of rooms that do not take into account cart proximity or input from workers. As a result, workers may have to push heavy cleaning carts across significantly greater distances and may be penalized for not meeting their room quota.⁴⁷ But an innovative collaboration between engineers at Carnegie Mellon University and hotel workers and their union resulted in a system redesign that would increase worker discretion, foster collaboration and communication, and reduce workloads.⁴⁸

The proposed regulations do not explicitly give workers and unions a role in risk assessments. While the proposed regulations could be read to imply that workers and unions should be consulted, we recommend the addition of the following text to Section 7151(a), to acknowledge the unique position and interests of workers and their unions.

In addition, when performing risk assessments of the processing of worker personal information or automated decisionmaking technologies impacting workers, a business should meaningfully consult with employees, independent contractors, and, if applicable, their exclusive bargaining representatives, including through participatory design, involvement in the identification of potential harms, and soliciting and incorporating feedback. These risk assessments should then be shared with employees, independent contractors, and, if applicable, their exclusive bargaining representatives.

⁴⁵ See Amanda Ballantyne, Jodi Forlizzi, and Crystal Weise, "A Vision for Centering Workers in Technology Development," Issues in Science and Technology (Fall 2024), and Thomas Kochan, et al. "Bringing Worker Voice Into Generative AI," Institute for Work and Employment Research, MIT Sloan School of Management (December 21, 2023).

⁴⁶ Adam Seth Litwin, "Technological Change at Work: The Impact of Employee Involvement on the Effectiveness of Health Information Technology," ILR Review 64, no. 5 (October 2011).

⁴⁷ Juliana Feliciano Reyes, "Hotel Housekeeping on Demand: Marriott Cleaners Say this App Makes their Job Harder," The Philadelphia Inquirer (July 2, 2018).

⁴⁸ Franchesca Spektor, et al., "Designing for Wellbeing: Worker-Generated Ideas on Adapting Algorithmic Management in the Hospitality Industry," Proceedings of the 2023 ACM Designing Interactive Systems Conference, 623–37 (2023).

Recommendation 6: Strengthen the power of the CCPA to act on risk assessments.

The risk assessment framework of the proposed regulations does not currently provide a clear regulatory mechanism for the Agency to disagree with a company's certification that the benefits of some processing activity outweigh the costs. This lack of authority risks hobbling the Agency's ability to prevent the most egregious privacy violations revealed by a business's risk assessment.

Risk assessments are required by the CCPA for a simple reason: when the costs associated with processing consumers' personal information outweigh the benefits, the processing should be restricted or prohibited outright. As the statute makes explicit, risk assessments weigh the risks "with the goal of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."

Regulations that only require risk assessments to be prepared by businesses and maintained internally are insufficient to protect the autonomy and dignity of the public from processing activities that do not meet the legal standard. Imagine a processing activity that risks significant harm to vulnerable consumers—like people searching for housing or employment—but which is marginally profitable for a business. When a business self-certifies that the processing's benefits outweigh the costs, it is the Agency's role under the statute to review the certification and the supporting analysis and determine whether it properly performs the cost-benefit analysis. If it does not, then the processing, under the CCPA, must be restricted or prohibited (see Civil Code § 1798.185(a)(15)(B)).

We propose the following language, based on the statutory damages provisions in § 1798.155(a), creating an explicit mechanism for the Agency to question and take action against deficient risk assessments:

Upon review of a business's Risk Assessment, if the Agency has a cause to conclude that the benefits of the processing do not outweigh the costs as required by statute, the Agency may require additional documentation or evidence from the business. If the Agency determines, after reviewing any further materials as necessary, that there is probable cause for believing that the benefits of the processing do not outweigh the costs in violation of the statute, the Agency may hold a hearing pursuant to Section 1798.199.55(a) to determine if a violation has occurred. If the Agency so determines that a violation has occurred, it may issue an order requiring the violator to restrict the processing to address such costs or prohibiting the business from such processing.

The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward. Full coverage and protection by the CCPA is a critical first step to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Thank you for the opportunity to provide feedback during this important rulemaking process,

Sincerely,
The signed organizations and individuals

Organizations:

Alphabet Workers Union - CWA Local 9009
American Civil Liberties Union California Action
American Federation of Musicians Local 7
Athena Coalition
California Coalition for Worker Power
California Conference Board of the Amalgamated Transit Union
California Conference of Machinists
California Employment Lawyers Association
California Federation of Labor Unions
California Immigrant Policy Center
California Nurses Association/National Nurses United
California School Employees Association
California Teamsters Public Affairs Council
CFT, A Union of Educators and Classified Professionals
Communications Workers of America (CWA)
Coworker
Data & Society
Distributed AI Research Institute
Economic Security California Action
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Equal Rights Advocates
Gig Workers Rising
Human Impact Partners
IBEW 569
Labor Occupational Health Program, UC Berkeley
Los Angeles Alliance for a New Economy (LAANE)
National Domestic Workers Alliance
National Employment Law Project
PowerSwitch Action
SAG-AFTRA
SEIU California
Strippers United
Surveillance Technology Oversight Project
TechEquity
TechTonic Justice
The Sidewalk Project
UC Berkeley Labor Center
UC San Diego Labor Center
UDW/AFSCME Local 3930
United Food and Commercial Workers (UFCW) Western States Council
United for Respect Education Fund
Upturn
Worksafe
Writers Guild of America West

Individuals (organizations listed for identification purposes only):

Zarreen Amin (SEIU-UHW)

Sameer Ashar (UC Irvine Workers, Law, and Organizing Clinic)

Christina Chung (Center for Law and Work, Berkeley Law School)

NatsHoney Clark (Strippers United)

Andrea Dehlendorf

Veena Dubal (University of California, Irvine School of Law)

Sarah Fox (Carnegie Mellon University)

Ifeoma Ozoma (Earthseed)

Seema Patel (UC College of the Law, San Francisco [formerly UC Hastings])

Kevin Riley (UCLA Labor Occupational Safety and Health Program)

From: [Antonia Crane](#)
To: Regulations@CPPA
Subject: Public Comment on Risk Assessments and ADMT
Date: Sunday, January 12, 2025 6:43:37 PM

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 11, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Board Members, Executive Director Soltani, and Agency Staff,

The Stripper Worker Center appreciates the opportunity to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act (CCPA). We commend Executive Director Soltani, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

For union and non-union workers alike, the emergence of AI and other data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, potentially affecting workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovations – and in particular, to ensure that workers have the ability to control the collection and use of their personal data.

We have signed onto a joint letter with detailed recommendations, that will be submitted under separate cover. In this letter, we would like to share with you stories from our worker members about how data-driven technologies are impacting their work lives, underscoring why fully protecting workers in these new regulations is so important.

They convey having received warnings about online content on their OnlyFans accounts.

We recommend the following:

- Strengthen the required elements of risk assessments.
- Clarify the role of workers and unions in risk assessments.
- Strengthen the power of the California Privacy Protection Agency to act on risk assessments
- Expand the definition of Automated Decision Making Technology to ensure that the new regulations fully protect workers.
- Strengthen notice and access rights for workers when an employer has used an ADMT to make a decision about them
- Restore a meaningful right for workers and consumers to opt-out of consequential ADMT systems.

The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward. Full coverage and protection by the CCPA is a critical first step to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Thank you for the opportunity to provide feedback during this important rulemaking process,

Sincerely,
Antonia Crane

--

[Antonia Crane](#)

Wallis Annenberg PhD Fellow in Creative Writing/Literature
University of Southern California

CEO/Founder: Stripper Worker Center 501(c)(4)
EIN 99-473-7973

A World Workers Built
STOP THE RAIDS



Regulations@CPPA

From: Tabitha Leonards <pals@strippersunited.org>
Sent: Friday, January 10, 2025 11:17 AM
To: Regulations@CPPA
Cc: Nats Honey; Glen Parker
Subject: Public Comment on Risk Assessments and ADMT

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 10, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Board Members, Executive Director Soltani, and Agency Staff,

Strippers United appreciates the opportunity to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act (CCPA). We commend Executive Director Soltani, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

For union and non-union workers alike, the emergence of AI and other data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, potentially affecting workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovations – and in particular, to ensure that workers have the ability to control the collection and use of their personal data.

We have signed onto a joint letter with detailed recommendations, that will be submitted under separate cover. In this letter, we would like to share with you stories from our worker members about how data-driven technologies are impacting their work lives, underscoring why fully protecting workers in these new regulations is so important.

My organization that advocated for stripper labor rights was deleted without any reason or warning. It was deep into the pandemic and our followers were relying on our site for mutual aid and for connection to their support systems. It was very troubling to imagine a security bot deciding that my community and myself were not worthy to exist online for arbitrary reasons. It took several days to retrieve our account, which only happened because my partner had insider tech friends who could make a call on our behalf.

The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward. Full coverage and protection by the CCPA is a critical first step to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Thank you for the opportunity to provide feedback during this important rulemaking process,

Sincerely,

Strippers United

pals@strippersunited.org

Regulations@CPPA

From: Tabitha Leonards <pals@strippersunited.org>
Sent: Friday, January 10, 2025 11:32 AM
To: Regulations@CPPA
Subject: Public Comment on Risk Assessments and ADMT

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 10, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Board Members, Executive Director Soltani, and Agency Staff,

Strippers United appreciates the opportunity to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act (CCPA). We commend Executive Director Soltani, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

For union and non-union workers alike, the emergence of AI and other data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, potentially affecting workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovations – and in particular, to ensure that workers have the ability to control the collection and use of their personal data.

We have signed onto a joint letter with detailed recommendations, that will be submitted under separate cover. In this letter, we would like to share with you stories from our worker members about how data-driven technologies are impacting their work lives, underscoring why fully protecting workers in these new regulations is so important.

My organization that advocated for stripper labor rights was deleted without any reason or warning. It was deep into the pandemic and our followers were relying on our site for mutual aid and for connection to their support systems. It was very troubling to imagine a security bot deciding that my community and myself were not worthy to exist online for arbitrary reasons. It took several days to retrieve our account, which only happened because my partner had insider tech friends who could make a call on our behalf.

We recommend the following:

- Strengthen the required elements of risk assessments.
- Clarify the role of workers and unions in risk assessments.
- Strengthen the power of the California Privacy Protection Agency to act on risk assessments
- Expand the definition of Automated Decisionmaking Technology to ensure that the new regulations fully protect workers.
- Strengthen notice and access rights for workers when an employer has used an ADMT to make a decision about them
- Restore a meaningful right for workers and consumers to opt-out of consequential ADMT systems.

The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward. Full coverage and protection by the CCPA is a critical first step to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Thank you for the opportunity to provide feedback during this important rulemaking process,

Sincerely,

Strippers United
pals@strippersunited.org

From: [Jeff](#)
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Date: Monday, January 13, 2025 6:54:31 AM
Attachments: [Jeff Bond CPPA Testimony.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 CPPA,

My name is Jeff Bond, and I'm a California-based small business owner (Founder, [Inspect.Net](#)). I'd like to submit the following comment to the CPPA for their consideration during the public hearing on January 14th.

Good morning, Chair Urban and Board Members.

Thank you for your efforts to keep Californians' data safe, and for giving me the chance to speak today. My business uses data-powered and ADMT tools to connect with customers and grow. I'll soon have over 100,000 annual website-hits, and I'm very worried about the impact of your proposed regulations.

My name is Jeff Bond, and I founded my home-inspection company, Inspect.Net, in 1992. I've helped 15,000 families from 100 countries purchase homes in the Bay area. I'm a trained engineer and a licensed contractor, and all my reports exceed home-inspection industry standards. I want to ensure families invest in homes that are safe and structurally sound.

Ninety percent of my customers find me online, thanks to data-powered and automated digital tools. I use targeted ads because I need to reach the specific segment of people considering buying a Bay-area property. I can't afford to waste money advertising to the general public. If people opt out of receiving automated data-driven ads — which they might do simply because they're annoyed with the proposed pop-up screens — I won't be able to reach the right audience. That will be disastrous for my business.

But it gets worse. Along with my ads, all my online marketing directs people to my website, which I've carefully designed to be as helpful and informative as possible. If people have to navigate multiple pop-ups en route to my site, they'll likely leave before they even have a chance to explore it.

If people don't visit my website, I'll go out of business. Obviously, that's really bad for me. But it's also really bad for potential buyers and home owners, who'll lose an experienced local inspector working directly for *them* — not an insurer or broker. And because California doesn't require home inspectors to be licensed, many people may end up working with someone dangerously inexperienced.

The proposed regulations fail to recognize that data-powered and automated tools offer many benefits. Targeted ads often help people find products and services they really need. And data-powered and ADMT tools help tiny businesses like mine successfully compete against much bigger players.

Finally, the 100,000 website-hits threshold punishes businesses that are growing and succeeding. As soon as I hit that threshold, I know I'll have to undertake an expensive website redesign and change my advertising and marketing tactics in ways that may put me out of business. That is not a fair or wise policy.

Please reconsider these regulations, which will badly hurt thousands of small California businesses. Thank you again for allowing me to speak today.

Sincerely,
Jeff Bond

--

Jeff Bond, President

Inspect.Net, Inc.

<https://youtu.be/gxqOex8IKyY>

Public Comment on Proposed ADMT Rulemaking Actions

California Privacy Protection Agency Public Hearing

January 14, 2025

Jeff Bond, founder, [Inspect.Net](https://inspect.net)

Hayward, CA

Good morning, Chair Urban and Board Members.

Thank you for your efforts to keep Californians' data safe, and for giving me the chance to speak today. My business uses data-powered and ADMT tools to connect with customers and grow. I'll soon have over 100,000 annual website-hits, and I'm very worried about the impact of your proposed regulations.

My name is Jeff Bond, and I founded my home-inspection company, Inspect.Net, in 1992. I've helped 15,000 families from 100 countries purchase homes in the Bay area. I'm a trained engineer and a licensed contractor, and all my reports exceed home-inspection industry standards. I want to ensure families invest in homes that are safe and structurally sound.

Ninety percent of my customers find me online, thanks to data-powered and automated digital tools. I use targeted ads because I need to reach the specific segment of people considering buying a Bay-area property. I can't afford to waste money advertising to the general public. If people opt out of receiving automated data-driven ads — which they might do simply because they're annoyed with the proposed pop-up screens — I won't be able to reach the right audience. That will be disastrous for my business.

But it gets worse. Along with my ads, all my online marketing directs people to my website, which I've carefully designed to be as helpful and informative as possible. If people have to navigate multiple pop-ups en route to my site, they'll likely leave before they even have a chance to explore it.

If people don't visit my website, I'll go out of business. Obviously, that's really bad for me. But it's also really bad for potential buyers and home owners, who'll lose an experienced local inspector working directly for *them* — not an insurer or broker. And because California doesn't require home inspectors to be licensed, many people may end up working with someone dangerously inexperienced.

The proposed regulations fail to recognize that data-powered and automated tools offer many benefits. Targeted ads often help people find products and services they really need. And data-powered and ADMT tools help tiny businesses like mine successfully compete against much bigger players.

Finally, the 100,000 website-hits threshold punishes businesses that are growing and succeeding. As soon as I hit that threshold, I know I'll have to undertake an expensive website redesign and change my advertising and marketing tactics in ways that may put me out of business. That is not a fair or wise policy.

Please reconsider these regulations, which will badly hurt thousands of small California businesses. Thank you again for allowing me to speak today.

From: [Anh Nguyen](#)
To: Regulations@CPPA
Cc: [Lisa Marroquin](#); [Nella McOsker](#)
Subject: Public Comment on Proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.
Date: Monday, January 13, 2025 2:25:29 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[CCA CCPA Comment Letter.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 the Central City Association's comments regarding the proposed CCPA Updates, Cyber, Risk, ADMT and Insurance Regulations. We appreciate the opportunity to submit and please let me know if you have any questions.



Anh Nguyen

Chief Strategy Officer

she/her | 213.416.7513 | anguyen@ccala.org |

ccala.org

626 Wilshire Blvd., Suite 850, Los Angeles, CA 90017

[CCA Reflects](#) |





January 13, 2024

California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Submitted via email at: regulations@coppa.ca.gov

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

To Whom It May Concern:

Established in 1924, Central City Association (CCA) represents approximately 300 member organizations committed to advancing policies and projects that enhance Downtown Los Angeles' vibrancy and increase economic opportunities. On behalf of CCA, I write to express our strong opposition to the proposed Automated Decision-Making Technology and Risk Assessment regulations. While we share 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 overly 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.

We ask that you carefully consider the problematic issues described below:

- The proposed ADMT/AI rules are well outside the scope of authority under the CCPA and are exceedingly broad and imprecise as written – more specifically, the automated decision-making tools. The proposed regulation to create a consumer opt-out of automated decision-making tools should be reconsidered as these tools are integral to a business' ability to do 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

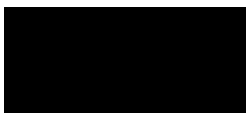


interest in purchasing. This would be an unnecessary expansion of privacy regulations into routine business practices that consumers generally find helpful, not harmful.

- Second, even though the regulations are focused on “automated decision-making” 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 software that simply help humans make decisions, rather than truly replacing 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.
- Third as currently drafted, Section 7123(f) should be reassessed. No other audit regime is comparable to the CCPA audit; thus, businesses will always be required to conduct a separate audit for CCPA. More helpful would be a list of common security audit frameworks that will be accepted as compliant. Relatedly, the specific controls in 7123(b) run the risk of quickly becoming outdated. Most existing cybersecurity audit standards call for the assessment of how organizations achieve particular outcomes. The CPPA’s proposal instead requires specific security controls to achieve certain outcomes. For example, (b)(2)(A) focuses on MFA and passwords when most companies are increasingly moving to passkeys.
- Finally, 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.

The proposed rules would create significant competitive disadvantages for California businesses. 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.

Sincerely,



Nella McOsker
President & CEO
Central City Association

From: [Peter Leroe-Muñoz](#)
To: Regulations@CPPA
Subject: Comments: Coalition of CA Business Associations and Chambers of Commerce
Date: Monday, January 13, 2025 5:32:53 PM
Attachments: [Jan 13 CPPA Draft Rules Coalition Letter.docx.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](#)

Hello,

Please find attached joint comments from a coalition of business associations and chambers of commerce throughout the state regarding the proposed regulations concerning, among other items, ADMT and AI.

Please advise of any questions.

Best,
Peter

Peter Leroe-Muñoz (He/Him/His)

General Counsel
SVP, Tech & Innovation

408.427.4697 | svlg.org

Connect with us: [Twitter](#) | [LinkedIn](#) | [Facebook](#)



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



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 Institute¹ 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 organizations³ 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 *overstates*, 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://coppa.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)	<p><i>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:</i></p> <p>“For purposes of this Article, “extensive profiling” means <u>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):</u>”</p>
#2	Deletion or revision of § 7150(b)(4)	<p><i>§ 7150(b)(4) should be deleted in its entirety, but if it is retained it should be revised, including as follows:</i></p> <p>“Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence that is capable of being <u>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)):</u>”</p>
#3	Revision of § 7200(a)	<p>“A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article, <u>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): . . .</u>”</p>

#4	Deletion or revision of § 7200(a)(2)	<p><i>§ 7200(a)(2) should be deleted in its entirety, but if it is retained it should be revised, including as follows:</i></p> <p><i>“For extensive profiling of a consumer. For purposes of this Article, “extensive profiling” means <u>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):</u>”</i></p>
#5	Deletion or revision of § 7200(a)(3)	<p><i>§ 7200(a)(3) should be deleted in its entirety, but if it is retained it should be revised, including as follows:</i></p> <p><i>“For training uses of automated decisionmaking technology, which are pProcessing consumers’ personal information to train automated decisionmaking technology that is capable of being <u>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)):</u>”</i></p>
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 <u>if the business is not subject to examination or supervision by a federal prudential regulator with respect to cybersecurity</u> 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 <u>unless the business is subject to examination or supervision by a federal prudential regulator with respect to cybersecurity.</u> ”

		“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 <u>or if a risk assessment is undertaken in a manner that is subject to examination or supervision by a federal prudential regulator.</u> ”
#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 <u>except to the extent undertaken in a manner that is subject to examination or supervision by a federal prudential regulator:</u> ”
#11	In the alternative, revision of § 7200(a) and addition of new § 7200(b)	<p>“A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article <u>except as set forth in subsection (b) below:</u>”</p> <p>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.”</p>
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)	<p>“‘Automated decisionmaking technology’ or ‘ADMT’ means any technology that processes solely automated processing of personal information <u>and uses computation to execute a decision which produces legal or similarly significant effects</u> or replace human decisionmaking, or substantially facilitate human decisionmaking.”</p> <p><u>or, in the alternative:</u></p> <p>“‘Automated decisionmaking technology’ or ‘ADMT’ means any technology that processes solely automated processing of personal information <u>and uses computation to execute a decision or</u> replace human decisionmaking, or substantially facilitate human decisionmaking.”</p>

		<i>In addition, the defined term “artificial intelligence” should be deleted in § 7001(c).</i>
#13	In the alternative, revision of § 7001(f)(4)	<p>“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.”</p>
#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)	<i>These provisions should be deleted in their entirety.</i>
#15	Revision of § 7200(a)	<p><i>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:</i></p> <p>“A business that uses automated decisionmaking technology <u>to make decisions about natural persons who are California residents</u> in any of the following ways must comply with the requirements of this Article: . . .”</p>

#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)	<p>“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 <u>for the purposes set forth in section 7200, subsection (a)</u> using that automated decisionmaking technology.”</p> <p>“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:</p> <p>(1) Ceasing to process the consumer’s personal information <u>for the purposes set forth in section 7200, subsection (a)</u> 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”</p>
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)	<p>“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:</p> <p>(1) The business’s use of that automated decisionmaking technology is <u>for necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes, including but not limited to the purposes</u> listed below (“security, fraud prevention, and safety exception”): (A) To prevent, detect, and</p>

		<p>investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information <u>or the availability, integrity, or confidentiality of information systems, or otherwise help ensure security and integrity of personal information or information systems</u>; (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; <u>(D) To otherwise ensure security and integrity; or (E) To comply with laws, including any regulation or guidance implementing such laws.</u>”</p> <p><i>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).</i></p>
#20	Revision of § 7221(b)(3)	<p><i>The Agency should also consider more appropriately scoping the other exemptions in its ADMT rule:</i></p> <p>“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:</p> <p>(A) The automated decisionmaking technology is <u>for necessary to achieve, and is used solely for</u>, 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 . . . “</p> <p><i>Corresponding revisions should be made to § 7221(b)(4) and (b)(5).</i></p>
#21	Revision of § 7221(b)(6)	<p>Deletion of this provision</p> <p><u>or</u></p> <p>“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.”</p>
#22	Revision of § 7221(g)	<p><i>The Agency must revise this provision to avoid forcing businesses to provide information to bad actors that they can use to further fraudulent activities:</i></p>

		“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 <u>500,000</u> 250,000 or more consumers or households in the preceding calendar year; or (B) Processed the sensitive personal information of <u>250,000</u> 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 <u>regularly, such as at least once every calendar year</u> , and there must be no gap in the months covered by successive cybersecurity audits. <i>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.</i>

#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. <u>This audit may be conducted using multiple audits, provided that the below requirements are satisfied across these audits.</u> ”
#27	Revision of § 7123(b)(2)	<p>“The cybersecurity audit must specifically identify, address, and document . . . Each of the following components of the business’s cybersecurity program, as applicable <u>and appropriate to the business’s size and complexity and the nature and scope of its processing activities.</u> If not applicable, the cybersecurity audit must document and explain <u>any comparable components relevant to the business’s protection of personal information</u> 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.”</p> <p><i>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).</i></p>
#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. <u>This description may be either general or specific to each of the requirements.</u> ”
#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)	<p>“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.”</p> <p><u>and</u></p>

		“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. <u>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.</u> ”
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, <u>in each case where relevant to the identified significant risk to consumers’ privacy and security: . . .</u> ”
#33	Revisions to § 7152(a)(1), 7152(a)(2), and 7152(a)(6) (among other revisions to decrease the	<p>“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.’”</p> <p>“The business must identify the categories of personal information to be processed and whether they include sensitive personal information. This must include <u>discussion of the following, as applicable:</u>”</p>

	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 <u>collectively</u> 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)	<p>“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), <u>in each case as material to the benefits, impacts, or effectiveness of the safeguards.</u></p> <p>Material changes may include, for example, <u>material</u> changes to the purpose of the processing; <u>material changes</u> to the minimum personal information necessary to achieve the purpose of the processing; or <u>material changes to the risks to consumers’ privacy</u> raised by consumers (e.g., numerous consumers complain to a business about the risks that the business’s processing poses to their privacy).”</p>
#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 <u>where there is a material change to the data processing</u> 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 <u>reasonably</u> 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 <u>reasonably</u> meet all of the requirements of this Article, the business <u>may</u> must supplement the risk assessment with any additional information required to meet all of the requirements of this Article.”
#37	Addition of § 7157(e)	<p><i>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:</i></p> <p>“Nothing in this Article 10 shall require a business to divulge trade secrets.”</p>

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





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