NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

DRAFT
RISK ASSESSMENT
and
AUTOMATED DECISIONMAKING TECHNOLOGY REGULATIONS

MARCH 2024

CPPA

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

[ADDITIONS TO] § 7001. Definitions.

"Artificial intelligence" means a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments. The artificial intelligence may do this to achieve explicit or implicit objectives. Outputs can include predictions, content, recommendations, or decisions. Different artificial intelligence varies in its levels of autonomy and adaptiveness after deployment. For example, artificial intelligence includes generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial- or speech-recognition or -detection technology.

"Automated decisionmaking technology" means any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.

(1) For purposes of this definition, "technology" includes software or programs, including those derived from machine learning, statistics, other data-processing techniques, or artificial intelligence.

(2) For purposes of this definition, to "substantially facilitate human decisionmaking" means using the output of the technology as a key factor in a human's decisionmaking. This includes, for example, using automated decisionmaking technology to generate a score about a consumer that the human reviewer uses as a primary factor to make a significant decision about them.

(3) Automated decisionmaking technology includes profiling.

(4) Automated decisionmaking technology does not include the following technologies, provided that the technologies do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking: web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies. A business must not use these technologies to circumvent the requirements for automated decisionmaking technology set forth in these regulations. For example, a business's use of formulas in a spreadsheet to determine which employees it will terminate is a use of automated decisionmaking technology subject to the requirements of this Article.

"Behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity—both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services.

(1) Behavioral advertising includes cross-context behavioral advertising.

(2) Behavioral advertising does not include nonpersonalized advertising, as defined by Civil Code section 1798.140, subdivision (t),[1] provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party.

"Deepfake" means manipulated or synthetic audio, image, or video content that depicts a consumer saying or doing things they did not say or do and that are presented as truthful or authentic without the consumer's knowledge and permission.

"Performance at work" means the performance of job duties for which the consumer has been hired or has applied to be hired. The following are not "performance at work": a consumer's union membership or interest in unionizing; a consumer's interest in seeking other employment opportunities; a consumer's location when off-duty or on breaks; or a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the business's information system or to prevent the disclosure of confidential information.

"Performance in an educational program" means the performance of coursework in an educational program in which the consumer is enrolled or has applied to be enrolled. The following are not "performance in an educational program": a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the educational program provider's information system, including to prevent the disclosure of confidential information or to prevent cheating; or a consumer's location when they not performing coursework.

[1] For ease of reference, Civil Code section 1798.140, subdivision (t) states the following: "Nonpersonalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

"Physical or biological identification or profiling" means identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body. This includes using biometric information, vocal intonation, facial expression, and gesture (e.g., to identify or infer emotion).

"Profiling" means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements.

"Publicly accessible place" means a place that is open to or serves the public. Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, transit, streets, or parks.

"Systematic observation" means methodical and regular or continuous observation. This includes, for example, methodical and regular or continuous observation using wi-fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, technologies that enable physical or biological identification or profiling; geofencing, location trackers, or license-plate recognition.

"Train automated decisionmaking technology or artificial intelligence" means the process through which automated decisionmaking technology or artificial intelligence discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. Examples of training include adjusting the parameters of an algorithm used for automated decisionmaking technology or artificial intelligence, improving the algorithm that determines how a machine-learning model learns, and iterating the datasets fed into automated decisionmaking technology or artificial intelligence.

[ADDITIONS TO] § 7050. Service Providers and Contractors.

(h) A service provider or contractor must, with respect to personal information that they collected pursuant to their written contract with the business, cooperate with the business in conducting the business's risk assessment pursuant to Article 10, including by making available to the business all facts necessary to conduct the risk assessment and not misrepresenting in any manner any fact necessary to conduct the risk assessment.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

[MODIFICATIONS TO] § 7051. Contract Requirements for Service Providers and Contractors.

[Green double-underline illustrates proposed additions to existing section 7051, subsection (a)(6).]

(a)(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, to assist the business in completing the business's cybersecurity audit pursuant to Article 9, to assist the business in conducting the business's risk assessment pursuant to Article 10, to assist the business in complying with the business's automated decisionmaking technology requirements pursuant to Article 11, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

[ADDITION] ARTICLE 10. RISK ASSESSMENTS

§ 7150. When a Business Must Conduct a Risk Assessment.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) must conduct a risk assessment before initiating that processing.

(b) Each of the following processing activities presents significant risk to consumers' privacy:

(1) Selling or sharing personal information.

(2) Processing sensitive personal information.

(A) A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for purposes of administering compensation payments, determining and storing employment authorization, administering health insurance and other benefits, or wage reporting as required by law, is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of

consumers' sensitive personal information is subject to the risk-assessment requirements set forth in this Article.

(3) Using automated decisionmaking technology for a significant decision concerning a consumer or for extensive profiling.

(A) For purposes of this Article, "significant decision" means a decision using 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), that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).

(i) Education enrollment or opportunity includes:

1. Admission or acceptance into academic or vocational programs;
2. Educational credentials (e.g., a degree, diploma, or certificate); and
3. Suspension and expulsion.

(ii) Employment or independent contracting opportunities or compensation includes:

1. Hiring;
2. Allocation or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits ("allocation/assignment of work and compensation");
3. Promotion; and
4. Demotion, suspension, and termination.

(B) For purposes of this Article, "extensive profiling" means:

(i) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job

applicant, student, employee, or independent contractor ("work or educational profiling");

(ii) Profiling a consumer through systematic observation of a publicly accessible place ("public profiling"); or

(iii) Profiling a consumer for behavioral advertising.

(4) Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence that is capable of being used for any of the following:

(A) For a significant decision concerning a consumer;

(B) To establish individual identity;

(C) For physical or biological identification or profiling;

(D) For the generation of a deepfake; or

(E) For the operation of generative models, such as large language models.

(c) Illustrative examples of when a business must conduct a risk assessment:

(1) Business A is a rideshare provider. Business A seeks to use automated decisionmaking technology to allocate rides and determine fares and bonuses for its drivers. Business A must conduct a risk assessment because it seeks to use automated decisionmaking technology for a significant decision concerning a consumer.

(2) Business B is hiring a new employee. Business B seeks to use emotion-assessment technology as part of the job interview process to determine who to hire. Business B must conduct a risk assessment because it seeks to use automated decisionmaking technology (specifically, physical or biological identification or profiling) for a significant decision concerning a consumer.

(3) Business C provides a mobile dating application. Business C seeks to disclose consumers' precise geolocation and the ethnicity and medical information the consumers provided in their dating profiles to Business C's analytics service provider. Business C must conduct a risk assessment because it seeks to process sensitive personal information of consumers.

(4) Business D provides a personal-budgeting application into which consumers enter their financial information, including income. Business D seeks to display advertisements to these consumers on different websites for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability. Business D must conduct a risk assessment because it seeks to conduct extensive profiling and share personal information.

(5) Business E is a grocery store chain. Business E seeks to process consumers' device media access control (MAC) addresses via wi-fi tracking to observe consumers' shopping patterns within its grocery stores. Business E must conduct a risk assessment because it seeks to profile consumers through systematic observation of a publicly accessible place.

(6) Business F is a technology provider. Business F seeks to extract faceprints from consumers' photographs to train Business F's facial-recognition technology. Business F must conduct a risk assessment because it seeks to process consumers' personal information to train automated decisionmaking technology or artificial intelligence that is capable of being used to establish individual identity.

§ 7151. Stakeholder Involvement for Risk Assessments.

(a) The business must ensure that relevant individuals prepare, contribute to, or review the risk assessment, based upon their level of involvement in the processing activity that is subject to the risk assessment. Relevant individuals are those whose job duties pertain to the processing activity. For example, relevant individuals may be part of the business's product, fraud-prevention, or compliance teams. These individuals must make good faith efforts to disclose all facts necessary to conduct the risk assessment and must not misrepresent in any manner any fact necessary to conduct the risk assessment.

(b) A risk assessment may involve external parties to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, for example, service providers, contractors, experts in detecting and mitigating bias in automated decisionmaking technology, a subset of the consumers whose personal information the business seeks to process, or stakeholders that represent consumers' or others' interests, including consumer advocacy organizations.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

---

§ 7152. Risk Assessment Requirements.

(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 set forth below:

(1) **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."

(2) **The business must identify the categories of personal information to be processed and whether they include sensitive personal information**. This must include:

(A) The minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.

(B) For uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3)–(4), the business must identify the actions the business has taken or any actions it plans to take to maintain the quality of personal information processed by the automated decisionmaking technology or artificial intelligence.

(i) "Quality of personal information" includes completeness, representativeness, timeliness, validity, accuracy, consistency; and reliability of the sources of the personal information for the business's proposed use of the automated decisionmaking technology or artificial intelligence.

(ii) Actions a business may take to ensure quality of personal information include: (1) identifying the source of the personal information and whether that source is reliable (or, if known, whether the original source of the personal information is reliable); (2) identifying how the personal information is relevant to the task being automated and how it is expected to be useful for the development, testing, and operation of the automated decisionmaking technology or artificial intelligence; (3) identifying whether the personal information contains sufficient breadth to address the range of real-world inputs the automated decisionmaking technology or artificial intelligence may encounter; and (4) identifying

how errors from data entry, machine processing, or other sources are measured and limited.

(3) **The business must identify the following operational elements of its processing**:

(A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.

(B) How long the business will retain each category of personal information, and any criteria used to determine that retention period.

(C) The relationship between the consumer and the business, including whether the consumer interacts with the business, how they do so (e.g., via websites, applications, or offline), and the nature of the interaction (e.g., to obtain a good or service from the business).

(D) The approximate number of consumers whose personal information the business seeks to process.

(E) What disclosures the business has made or plans to make to the consumer about the processing, how these disclosures were made (e.g., via a just-in-time notice), and what actions the business has taken or plans to take to make these disclosures specific, explicit, prominent, and clear to the consumer.

(F) The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; the purpose for which the business discloses or makes the consumers' personal information available to them; and what actions the business has taken or plans to take to make consumers aware of the involvement of these entities in the processing.

(G) The technology to be used in the processing. For the uses of automated decisionmaking technology set forth in section 7150, subsections (b)(3), the business must identify:

(i) The logic of the automated decisionmaking technology, including any assumptions of the logic; and

(ii) The output of the automated decisionmaking technology, and how the business will use the output.

(4) **The business must specifically identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information**. For example, a business must not identify a benefit as "improving our service," because this does not identify the specific improvements to the service nor how the benefit resulted from the processing. If the benefit resulting from the processing is that the business profits monetarily (e.g., from the sale or sharing of consumers' personal information), the business must identify this benefit and, when possible, estimate the expected profit.

(5) **The business must specifically identify the negative impacts to consumers' privacy associated with the processing.** The business must identify the sources and causes of these negative impacts, and any criteria that the business used to make these determinations.

Negative impacts to consumers' privacy that a business may consider include the following:

(A) Unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information.

(B) Discrimination upon the basis of protected classes that would violate federal or state antidiscrimination law.

(C) Impairing consumers' control over their personal information, such as by providing insufficient information for consumers to make an informed decision regarding the processing of their personal information, or by interfering with consumers' ability to make choices consistent with their reasonable expectations.

(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.

(E) Disclosing a consumer's media consumption (e.g., books they have read or videos they have watched) in a manner that chills or deters their speech, expression, or exploration of ideas.

(F) Economic harms, including limiting or depriving consumers of economic opportunities; 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.

(H) Reputational harms, including stigmatization, that would negatively impact an average consumer. Examples of processing activities that result in such harms include a mobile dating application's disclosure of a consumer's sexual or other preferences in a partner; a business stating or implying that a consumer has committed a crime without verifying this information; or a business processing consumers' biometric information to create a deepfake of them.

(I) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation, that would negatively impact an average consumer. Examples of such harms include emotional distress resulting from disclosure of nonconsensual intimate imagery; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

(6) **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 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.

(A) Safeguards that a business may consider include the following:

(i) Encryption, segmentation of information systems, physical and logical access controls, change management, network monitoring and defenses, and data and integrity monitoring;

(ii) Use of privacy-enhancing technologies, such as trusted execution environments, federated learning, homomorphic encryption, and differential privacy;

(iii) Consulting external parties, such as those described in section 7151, subsection (b), to ensure that the business maintains current knowledge of emergent privacy risks and countermeasures; and using that knowledge to identify, assess, and mitigate risks to consumers' privacy; and

(iv) Evaluating the need for human involvement as part of the business's use of automated decisionmaking technology, and implementing policies, procedures, and training to address the degree and details of human involvement identified as necessary in that evaluation.

(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 ("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 ("accuracy and nondiscrimination safeguards"). For example, if a business determines that the use of low-quality enrollment images creates a high risk of false-positive matches in its proposed use of facial-recognition technology, the business must identify the policies, procedures, and training it has implemented or plans to implement to ensure that it is using only sufficiently high-quality enrollment images to mitigate that risk.

(iii) Where a business obtains the automated decisionmaking technology from another person, the business must identify the following:

1. Whether it reviewed that person's evaluation of the automated decisionmaking technology, and whether that person's evaluation included any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology.

2. Any accuracy and nondiscrimination safeguards that it implemented or plans to implement.

(7) **The business must identify whether it will initiate the processing subject to the risk assessment.**

(8) **The business must identify the contributors to the risk assessment**. In the risk assessment or in a separate document maintained by the business, the business must identify the individuals within the business and the external parties that contributed to the risk assessment.

(9) **The business must identify the date the assessment was reviewed and approved, and the names and positions of the individuals responsible for the review and approval.** The individuals responsible for the review and approval must include the individual who decides whether the business will initiate the processing that is subject to the risk assessment. If the business presented or summarized its risk assessment to the business's board of directors or governing body for review, or if no such board or equivalent body exists, to the business's highest-ranking executive who is responsible for oversight of risk-assessment compliance for review, the business must include the date of that review.

§ 7153. Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology or Artificial Intelligence.

(a) A business that makes automated decisionmaking technology or artificial intelligence available to another business ("recipient-business") for any processing activity set forth in section 7150, subsection (b), must provide all facts necessary to the recipient-business for the recipient-business to conduct its own risk assessment.

(b) A business that trains automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsection (b)(4) and permits another person to use that automated decisionmaking technology or artificial intelligence, must provide to the person a

plain language explanation of any requirements or limitations that the business identified as relevant to the permitted use of automated decisionmaking technology or artificial intelligence.

(c) The requirements of this section apply only to automated decisionmaking technology and artificial intelligence trained using personal information.

§ 7154. Prohibition Against Processing If Risks to Consumers' Privacy Outweigh Benefits.

(a) The business must not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing.

§ 7155. Timing and Retention Requirements for Risk Assessments.

(a) A business must comply with the following timing requirements for conducting and updating its risk assessments:

(1) A business must conduct and document a risk assessment in accordance with the requirements of this Article before initiating any processing activity identified in section 7150, subsection (b).

(2) At least once every three years, a business must review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.

(3) Notwithstanding subsection (a)(2) of this section, a business must immediately update a risk assessment whenever there is a material change relating to the processing activity. A change relating to the processing activity is material if it diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4), creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).

Material changes may include, for example, changes to the purpose of the processing; the minimum personal information necessary to achieve the purpose of the processing; or the risks to consumers' privacy raised by consumers (e.g., numerous consumers complain to a business about the risks that the business's processing poses to their privacy).

(b) A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.

(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 within 24 months of the effective date of these regulations.

§ 7156. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

(a) A business may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy.

(1) For example, Business G sells toys to children and is considering using in-store paper forms to collect names, mailing addresses, and birthdays from children that visit their stores, and to use that information to mail a coupon and list of age-appropriate toys to each child during the child's birth month and every November. Business G uses the same service providers and technology for each category of mailings across all stores. Business G must conduct and document a risk assessment because it is processing sensitive personal information. Business G may use a single risk assessment for processing the personal information for the birthday mailing and November mailing across all stores because in each case it is collecting the same personal information in the same way for the purpose of sending coupons and age-appropriate toy lists to children, and this processing presents similar risks to consumers' privacy.

(b) If the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that 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 meet all of the requirements of this Article, the business must supplement the risk assessment with any additional information required to meet all of the requirements of this Article.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

---

§ 7157. Submission of Risk Assessments to the Agency.

(a) **Timing of Risk Assessment Submissions.**

(1) **First Submission.** A business shall have 24 months from the effective date of these regulations to submit the risk assessment materials regarding the risk assessments that it has conducted from the effective date of these regulations to the date of submission ("first submission"). The risk assessment materials are set forth in subsection (b) and must be submitted to the Agency as set forth in subsection (c).

(2) **Annual Submission.** After the business completes its first submission to the Agency as set forth in subsection (a)(1), its subsequent risk assessment materials must be submitted every calendar year to the Agency, and there must be no gap in the months covered by successive submissions of risk assessment materials ("subsequent annual submissions").

(b) **Risk Assessment Materials to Be Submitted.** The first submission and subsequent annual submissions of the risk assessment materials to the Agency must include the following:

(1) **Certification of Compliance.** The business must submit a written certification that the business complied with the requirements set forth in this Article during the months covered by the first submission and subsequent annual submissions to the Agency on a form provided by the Agency.

(A) The business must designate a qualified individual with authority to certify compliance on behalf of the business. This individual must be the business's highest-ranking executive who is responsible for oversight of the business's risk-assessment compliance in accordance with this Article ("designated executive").

(B) The written certification must include:

(i) Identification of the months covered by the submission period for which the business is certifying compliance and the number of risk assessments that the business conducted and documented during that submission period;

(ii) An attestation that the designated executive has reviewed, understood, and approved the business's risk assessments that were conducted and documented in compliance with this Article;

(iii) An attestation that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment in compliance with this Article; and

(iv) The designated executive's name, title, and signature, and the date of certification.

(2) **Risk Assessments in Abridged Form:** For each risk assessment conducted and documented or updated by the business during the submission period, the business must submit an abridged version of the new or updated risk assessment to the Agency on a form provided by the Agency that includes:

(A) Identification of the processing activity in section 7150, subsection (b), that triggered the risk assessment;

(B) A plain language explanation of its purpose for processing consumers' personal information; and

(C) The categories of personal information processed, and whether they include sensitive personal information.

(3) **Risk Assessments in Unabridged Form:** A business also may include in its submission to the Agency a hyperlink that, if clicked, will lead to a public webpage that contains its unabridged risk assessment.

(4) **Exemptions.**

(A) 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.

(B) If a business previously conducted a risk assessment for a processing activity in compliance with this Article and submitted an abridged risk assessment to the Agency, and there were no material changes to that processing during a subsequent submission period, the business is not required to submit an updated risk assessment to the Agency. The business must still submit a certification of compliance to the Agency.

(c) **Method of Submission.** The risk assessment materials must be submitted to the Agency through the Agency's website.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

(d) **Risk Assessments Must Be Provided to the Agency or to the Attorney General Upon Request.** The Agency or the Attorney General may require a business to provide its unabridged risk assessments to the Agency or to the Attorney General at any time. A business must provide its unabridged risk assessments within 10 business days of the Agency's or the Attorney General's request.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

[ADDITION] ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

§ 7200. Uses of Automated Decisionmaking Technology.

(a) A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article:

(1) **For a significant decision concerning a consumer**.

(A) For purposes of this Article, "significant decision" means a decision using 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), that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).

(i) Education enrollment or opportunity includes:

1. Admission or acceptance into academic or vocational programs;
2. Educational credentials (e.g., a degree, diploma, or certificate); and
3. Suspension and expulsion.

(ii) Employment or independent contracting opportunities or compensation includes:

1. Hiring;
2. Allocation or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits ("allocation/assignment of work and compensation");
3. Promotion; and
4. Demotion, suspension, and termination.

(2) **For extensive profiling of a consumer**.

(A) For purposes of this Article, "extensive profiling" means:

(i) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ("work or educational profiling");

(ii) Profiling a consumer through systematic observation of a publicly accessible place ("public profiling"); or

(iii) Profiling a consumer for behavioral advertising.

(3) **For training uses of automated decisionmaking technology**, which includes processing consumers' personal information to train automated decisionmaking technology that is capable of being used for any of the following:

(A) For a significant decision concerning a consumer;

(B) To establish individual identity;

(C) For physical or biological identification or profiling; or

(D) For the generation of a deepfake.

§ 7201. Requirement for Physical or Biological Identification or Profiling.

(a) A business that uses physical or biological identification or profiling for a significant decision concerning a consumer as set forth in section 7200, subsection (a)(1), or for extensive profiling of a consumer as set forth in section 7200, subsection (a)(2), must comply with subsections (1) and (2) below:

(1) The business must conduct an evaluation of the physical or biological identification or profiling to ensure that it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the physical or biological identification or profiling technology"). For example, a business that uses emotion-assessment technology on its customer service calls to analyze the customer service employees' performance at work must conduct an evaluation to ensure that it works as intended for this use and does not discriminate based upon protected classes.

(A) Alternatively, where a business obtains the physical or biological identification or profiling technology from another person, the business must review that person's evaluation of the physical or biological identification or

profiling technology, including any requirements or limitations relevant to the business's proposed use of the physical or biological identification or profiling technology.

(2) The business must implement policies, procedures, and training to ensure that the physical or biological identification or profiling works as intended for the business's proposed use and does not discriminate based upon protected classes.

§ 7220. Pre-use Notice Requirements.

(a) A business that uses automated decisionmaking technology as set forth in section 7200, subsection (a), must provide consumers with a Pre-use Notice. The Pre-use Notice must inform consumers about the business's use of automated decisionmaking technology and consumers' rights to opt-out of, and to access information about, the business's use of automated decisionmaking technology, as set forth in this section.

(b) The Pre-use Notice must:

(1) Comply with section 7003;

(2) Be presented prominently and conspicuously to the consumer before the business processes the consumer's personal information using automated decisionmaking technology;

(3) Be presented in the manner in which the business primarily interacts with the consumer;

(4) Include the following:

(A) **A plain language explanation of the specific purpose for which the business proposes to use the automated decisionmaking technology.** The business must not describe the purpose in generic terms, such as "to improve our services."

(i) For training uses of automated decisionmaking technology set forth in section 7200, subsection (a)(3), the business must identify for which specific uses the automated decisionmaking technology is capable of being used, as set forth in section 7200, subsections (a)(3)(A)–(D). The business also must identify the categories of the consumer's personal information, including any sensitive personal information, that the business proposes to process for these training uses.

(B) **A description of the consumer's right to opt-out of the business's use of the automated decisionmaking technology and how the consumer can submit a request to opt-out of the business's use of the automated decisionmaking technology.**

(i) If the business is not required to provide the ability to opt-out because it is relying upon the human appeal exception set forth in section 7221, subsection (b)(2), the business must instead inform the consumer of their ability to appeal the decision and provide instructions to the consumer on how to submit their appeal.

(ii) If the business is not required to provide the ability to opt-out because it is relying upon another exception set forth in section 7221, subsection (b), the business must identify the specific exception it is relying upon.

(C) **A description of the consumer's right to access information** about the business's use of the automated decisionmaking technology with respect to the consumer and how the consumer can submit their access request to the business.

(i) If the business proposes to use automated decisionmaking technology solely for training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3), the business is not required to include a description about the right to access set forth in this subsection.

(D) **That the business is prohibited from retaliating against consumers for exercising their CCPA rights.**

(E) **Additional information about how the automated decisionmaking technology works.** The business may provide this information via a simple and easy-to-use method (e.g., a layered notice or hyperlink). The additional information must include a plain language explanation of the following:

(i) The logic used in the automated decisionmaking technology, including the key parameters that affect the output of the automated decisionmaking technology; and

1. For purposes of this Article, "output" includes predictions, content, and recommendations (e.g., numerical scores of compatibility).

(ii) The intended output of the automated decisionmaking technology and how the business plans to use the output, including the role of any human involvement. Illustrative examples follow:

1. If the business proposes to use the automated decisionmaking technology to make a significant decision concerning a consumer, the intended output may be a numerical score of compatibility, which a human may use as a key factor to make a hiring decision.

2. If the business proposes to use the automated decisionmaking technology for profiling for behavioral advertising, the intended output may be the placement of a consumer into a profile segment or category, which the business may use to determine which advertisements it will display to a consumer.

(iii) A business relying upon the security, fraud prevention, and safety exception to providing a consumer with the ability to opt out as set forth in section 7221, subsection (b)(1), is not required to provide information that would compromise its use of automated decisionmaking technology for these security, fraud prevention, or safety purposes when complying with this subsection.

(iv) If the business proposes to use automated decisionmaking technology solely for training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3), the business is not required to include the additional information set forth in this subsection.

(c) **A business may provide a consolidated Pre-use Notice as set forth below**, provided that the consolidated Pre-use Notice includes the information required by this Article for each of the business's proposed uses of automated decisionmaking technology:

(1) **The business's use of a single automated decisionmaking technology for multiple purposes.** For example, an employer may provide a consolidated Pre-use Notice to an employee that addresses the employer's proposed use of productivity monitoring software, which the employer also intends to use as a primary factor in determining the employee's allocation/assignment of work and compensation as set forth in section 7200, subsection (a)(1)(A)(ii)(2).

(2) **The business's use of multiple automated decisionmaking technologies for a single purpose.** For example, a business may provide a consolidated Pre-use Notice to a consumer that addresses the business's proposed use of public profiling as set forth in section 7200, subsection (a)(2)(A)(ii). The consolidated Pre-use Notice may address the business's proposed use of location trackers and facial-recognition technology to ensure the physical safety of natural persons.

(3) **The business's use of multiple automated decisionmaking technologies for multiple purposes.** For example, an educational provider may provide a consolidated Pre-use Notice to a new student that addresses the educational provider's proposed use of: (1) facial-recognition technology to authenticate the student and grant them access to a secured classroom, and (2) software that automatically screens a student's work for plagiarism.

(4) **The systematic use of a single automated decisionmaking technology.** For example, a business may provide a consolidated Pre-use Notice to an independent contractor that addresses the business's methodical and regular use of automated decisionmaking technology to allocate work to its independent contractors, rather than the business providing a Pre-use Notice each time it proposes to use the same automated decisionmaking technology to the same consumers for the same purpose.

§ 7221. Requests to Opt-Out of the Business's Use of Automated Decisionmaking Technology.

(a) Consumers shall have a right to opt-out of the business's use of automated decisionmaking technology as set forth in section 7200, subsection (a). A business must provide consumers with the ability to opt-out of these uses of automated decisionmaking technology, except as set forth in subsection (b).

(b) 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)(i); or for public profiling as set forth in section 7200, subsection (a)(2)(A)(ii), in the following circumstances:

(1) The business's use of that automated decisionmaking technology is necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below ("security, fraud prevention, and safety exception"):

(A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;

(B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or

(C) To ensure the physical safety of natural persons.

(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 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 is qualified to understand the significant decision being appealed and the consequences of the decision for the consumer. 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.

(B) The business must clearly describe to the consumer how to submit an appeal and enable the consumer to provide information for the human reviewer to consider as part of the appeal. The method of appeal also must be easy for the consumers to execute, require minimal steps, and comply with section 7004. Disclosures and communications with consumers concerning the appeal must comply with section 7003(a)–(b). [Staff recommends modifying existing regulation section 7021 (Timelines) to incorporate requests to appeal.]

(3) For admission, acceptance, or hiring decisions as set forth in section 7200, subsections (a)(1)(A)(i)(1), (a)(1)(A)(ii)(1), if the following are true:

(A) The automated decisionmaking technology is necessary to achieve, and is used solely for, the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and

(B) The business has conducted an evaluation of the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of

the automated decisionmaking technology"), and has implemented policies, procedures, and training to ensure that the automated decisionmaking technology works as intended for the business's proposed use and does not discriminate based upon protected classes ("accuracy and nondiscrimination safeguards").

(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.

(4) For allocation/assignment of work and compensation decisions as set forth in section 7200, subsection (a)(1)(A)(ii)(2), if the following are true:

(A) The automated decisionmaking technology is necessary to achieve, and is used solely for, the business's allocation/assignment of work or compensation; and

(B) The business has conducted an evaluation of the automated decisionmaking technology and has implemented accuracy and nondiscrimination safeguards.

(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.

(5) For work or educational profiling as set forth in section 7200, subsections (a)(2)(A)(i), if the following are true:

(A) The automated decisionmaking technology is necessary to achieve, and is used solely for, an assessment of the consumer's ability to perform at work or in an educational program, or their actual performance at work or in an educational program; and

(B) The business has conducted an evaluation of the automated decisionmaking technology and has implemented accuracy and nondiscrimination safeguards.

(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.

(6) **The exceptions in this subsection do not apply to profiling for behavioral advertising as set forth in section 7200, subsection (a)(2)(A)(iii), or to training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3).** A business shall provide the ability to opt-out of these uses of automated decisionmaking technology in all circumstances.

(c) A business that uses automated decisionmaking technology as set forth in subsection (a) must provide two or more designated methods for submitting requests to opt-out of the business's use of the automated decisionmaking technology. A business must consider the methods by which it interacts with consumers, the manner in which the business uses the automated decisionmaking technology, and the ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of the business's use of the automated decisionmaking technology. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. Illustrative examples and requirements follow.

(1) A business that interacts with consumers online must, at a minimum, allow consumers to submit requests to opt-out through an interactive form accessible via an opt-out link that is provided in the Pre-use Notice. The link must be titled [Note: Agency staff recommends receiving public comment on what the link(s) should be titled for consumers to understand the scope of the opt-out right].

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out in addition to the online form.

(3) Other methods for submitting requests to opt-out include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of the business's use of automated decisionmaking technology because cookies concern the

collection of personal information and not necessarily the use of automated decisionmaking technology. An acceptable method for submitting requests to opt-out must be specific to the right to opt-out of the business's use of the automated decisionmaking technology.

(d) A business's methods for submitting requests to opt-out of the business's use of the automated decisionmaking technology must be easy for consumers to execute, must require minimal steps, and must comply with section 7004.

(e) A business must not require a consumer submitting a request to opt-out of the business's use of the automated decisionmaking technology to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer.

(f) A business must not require a verifiable consumer request for a request to opt-out set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of automated decisionmaking technology. However, to the extent that the business can comply with a request to opt-out without additional information, it must do so.

(g) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of the business's use of the automated decisionmaking technology 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.

(h) A business must provide a means by which the consumer can confirm that the business has processed their request to opt-out of the business's use of the automated decisionmaking technology.

(i) In responding to a request to opt-out of the business's use of automated decisionmaking technology, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology as long as the business also offers a single option to opt-out of all of the business's uses of automated decisionmaking technology set forth in subsection (a).

(j) A consumer may use an authorized agent to submit a request to opt-out of the business's use of the automated decisionmaking technology as set forth in subsection (a) 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.

(k) Except as allowed by these regulations, a business must wait at least 12 months from the date the business receives the consumer's request to opt-out of the business's use of the automated decisionmaking technology before asking a consumer who has exercised their right to opt-out, to consent to the business's use of the automated decisionmaking technology for which the consumer previously opted out.

(l) If the consumer submits a request to opt-out of the business's use of the automated decisionmaking technology before the business has initiated that processing, the business must not initiate processing of the consumer's personal information using that automated decisionmaking technology.

(m) If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out after the business initiated the processing, the business must comply with the consumer's opt-out request by:

(1) Ceasing to process the consumer's personal information 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

(2) Notifying all the business's service providers, contractors, or other persons to whom the business has disclosed or made personal information available to process the consumer's personal information using that automated decisionmaking technology, that the consumer has made a request to opt-out and instructing them to comply with the consumer's request to opt-out of the business's use of that automated decisionmaking technology within the same time frame.

§ 7222. Requests to Access Information About the Business's Use of Automated Decisionmaking Technology.

(a) Consumers have a right to access information about the business's uses of automated decisionmaking technology that are set forth in sections 7200, subsections (a)(1)–(2), ("access right" or "right to access").

(1) A business that uses automated decisionmaking technology solely for training uses of automated decisionmaking technology, as set forth in section 7200, subsection (a)(3), is not required to provide a response to a consumer's request to access information about the business's use of the automated decisionmaking technology. The business must still comply with section 7024 ["Requests to Know"].

(b) **When responding to a consumer's request to exercise their access right, a business must provide plain language explanations of the following information to the consumer:**

(1) **The specific purpose for which the business used automated decisionmaking technology with respect to the consumer.** The business must not describe the purpose in generic terms, such as "to improve our services."

(2) **The output of the automated decisionmaking technology with respect to the consumer.** If the business has multiple outputs with respect to the consumer, the business may provide a simple and easy-to-use method by which the consumer can access all of the outputs.

(3) **How the business used the output with respect to the consumer.**

(A) If the business used the output of the automated decisionmaking technology to make a significant decision concerning the consumer as set forth in section 7200, subsection (a)(1), this explanation must include the role the output played in the business's decision and the role of any human involvement.

(i) If the business also plans to use the output to make a significant decision concerning the consumer as set forth in section 7200, subsection (a)(1), the business's explanation must additionally include how the business plans to use the output to make a decision with respect to the consumer, and the role of any human involvement.

(B) If the business used automated decisionmaking technology to engage in extensive profiling of the consumer as set forth in section 7200, subsection (a)(2), this explanation must include the role the output played in the evaluation that the business made with respect to the consumer.

(i) If the business also plans to use the output to evaluate the consumer as set forth in section 7200, subsection (a)(2), the business's explanation must additionally include how the business plans to use the output to evaluate the consumer.

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

(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.

(D) A business relying upon the security, fraud prevention, and safety exception to providing a consumer with the ability to opt-out as set forth in section 7221, subsection (b)(1), is not required to provide information that would compromise its use of automated decisionmaking technology for these security, fraud prevention, or safety purposes.

(5) That the business is prohibited from retaliating against consumers for exercising their CCPA rights, and instructions for how the consumer can exercise their other CCPA rights. These instructions must include any links to an online request form or portal for making such a request, if offered by the business.

(A) The business may comply with the instructions requirement by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains these instructions. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain these instructions, so that the consumer is required to scroll through other information in order to find the instructions, does not satisfy the instructions requirement.

(c) A business's methods for consumers to submit requests to exercise their access right ("access request" or "request to access") must comply with section 7020. [Staff recommends modifying existing regulation section 7020 to address the access right.]

(d) A business must respond to a request to access as soon as feasibly possible but no later than 45 calendar days from the date the business receives the request.

(e) A business must verify the identity of the person making the request to access as set forth in Article 5. If a business cannot verify the identity of the person making the request to access, the business must inform the requestor that it cannot verify their identity. [Staff recommends modifying existing Article 5 to incorporate verification requirements for the access right.]

(f) If a business denies a consumer's verified request to exercise their right to access, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business must inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer.

(g) A business must use reasonable security measures when transmitting the requested information to the consumer.

(h) If a business maintains a password-protected account with the consumer, it may comply with an access request by using a secure self-service portal for consumers to access, view, and receive a portable copy of their requested information if the portal fully discloses the requested information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

(i) A service provider or contractor must provide assistance to the business in responding to a verifiable consumer request to access, including by providing the business with the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

(j) A business that used an automated decisionmaking technology with respect to a consumer more than four times within a 12-month period may provide an aggregate-level response to the consumer's access request. Specifically, for the information required by subsections (b)(2)–(4), the business may provide a summary of the outputs with respect to the consumer over the preceding 12 months; the key parameters that, on average over the preceding 12 months, affected the outputs with respect to the consumer; and a summary of how those parameters generally applied to the consumer.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. This draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

(k) **Additional notice requirement regarding the access right when a business used automated decisionmaking technology for certain significant decisions.** A business that used automated decisionmaking technology to make certain significant decisions that were adverse to the consumer ("adverse significant decision"), as set forth in subsection (1) below, must provide the consumer with notice of their access right as set forth in subsection (2) below, as soon as feasibly possible but no later than 15 business days from the date of the adverse significant decision.

(1) A significant decision concerning a consumer that was adverse to the consumer is a significant decision that:

(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, or expelled; or

(B) Resulted in a consumer being denied financial or lending services, housing, insurance, criminal justice, healthcare services, or essential goods or services.

(2) The information that a business must provide to the consumer in this notice of their access right must include:

(A) That the business used automated decisionmaking technology to make the significant decision with respect to the consumer;

(B) That the business is prohibited from retaliating against consumers for exercising their CCPA rights;

(C) That the consumer has a right to access information about the business's use of the automated decisionmaking technology and how the consumer can exercise their access right; and

(D) If the business is relying upon the human appeal exception set forth in section 7221, subsection (b)(2), that the consumer can appeal the decision and how the consumer can submit their appeal and any supporting documentation.

(3) If a business provides notice to consumers of adverse significant decisions in its ordinary course (e.g., a business ordinarily notifies consumers of termination decisions via email), the business may include the information required by subsection (2) in that notice, provided that the notice overall complies with the requirements of

section 7003. Alternatively, a business may provide a separate contemporaneous notice of the consumer's access right that includes the information set forth in subsection (2).