A BILL

To preserve America's innovation engine; protect individuals' interests in the fair, ethical, transparent, and responsible processing of their personal data; mitigate risks of adverse impacts from the processing of personal data; and promote the benefits of the 21st century information age through an agile regulatory framework that contemplates that: (1) the sensitivity and value of data are increasingly difficult to understand and predict and (2) the majority of data about individuals is collected passively and observed through machine-to-machine transactions or computationally inferred.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Article I. SHORT TITLE AND TABLE OF CONTENTS

Section 1.01 SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Fair Accountable Innovative Responsible and Open Processing Enabling New Uses that are Secure and Ethical Act" or the "FAIR and OPEN USE Act".

(b) TABLE OF CONTENTS.—

Section 1.02 FINDINGS AND PURPOSE.

(a) The information ecosystem in the United States is the world's most innovative. It has not just driven economic growth; it has facilitated positive changes in all sectors.

(b) Data, including personal data about an individual, constitutes the lifeblood of the information age by forming the basic building blocks of all business, government, and social processes. Data provides unprecedented opportunities to drive information-based innovation in health care, public safety, education, transportation, and almost every human endeavor.

(c) Sensors, artificial intelligence, machine learning, and advanced analytics are now mainstays of our digital environment. These groundbreaking technologies extract value from data beyond that of the initial use and create new knowledge in ways once thought impossible. In a world of artificial intelligence, the systems themselves make decisions that impact people. The systems make decisions, based on human set objectives, but the direct human accountability has been lost.

(d) These technologies can have an adverse impact on an individual and cause negative impact on societal goals and values. The rapid growth of innovative, data-driven technologies has increased angst in individuals and a sense that they may be harmed by the misuse of information from them or about them. This concern is justified. Uses of personal data create risk to both individuals and society unless effective governance is in place and organizations are accountable for their actions.

(e) Increasingly, personal data is not collected directly from the individual but, rather, from a diverse range of sources without the individual's awareness of its origination and subsequent uses.

(f) The benefits of the information age belong to everyone. Individuals justifiably expect that organizations will process their data in a manner that creates benefits for the individual or, if not for the individual, for a broader community of people. Data should not just serve the interests of the organization that collected the data.

(g) Data use should support the value of human dignity—that an individual has an innate right to be valued, respected, and to receive ethical treatment. An individual should not be subject to secret processing of data that pertains to or will have an impact on the individual.

(h) Personal data must be kept secure. Too many organizations fail to protect sensitive personal data, undermining trust and confidence in the digital economy.

(i) The United States needs a new national framework addressing the processing of personal data that maintains the ability to think and learn from data while also protecting individuals in a highly observational digital ecosystem.

(j) Many legal frameworks today are structured as a list of prohibitions. This approach may lead to legal certainty by creating white lists and black lists of activities. However, since data use is dynamic, lists of prohibited activities lead to legal structures that are often dated when they go into effect. Moreover, such an approach may be unnecessarily restrictive while providing limited benefit or safeguards to individuals.

(k) We live in a complex, data-driven world with diverse business models and infinite possibilities for innovation. This reality requires an equally complex, nuanced, innovative, and agile policy and regulatory response. We cannot pretend that difficult digital challenges that evolve in real time can be solved with a short, simple legislative solution. We must embrace complexity, not run from it.

(l) A future-oriented legal framework must take into account the rapid evolution of data, technology, and business processes. It must preserve the ability of all entities to use data to pursue knowledge and should focus on flexible principles, not rigid prohibitions. It must be scalable to organizations of all sizes and complexities and be equally applicable to every sector of our global, digital economy.

(m) Data use must be—

(1) legal, the data used in a specific manner is specifically authorized or not prohibited;

(2) fair, data is used in a manner that maximizes stakeholder interests and mitigates risks to the extent possible; and

(3) just, inappropriate discrimination should be avoided even if the outcomes are maximized for many stakeholders.

(n) In today's data-driven economy, organizations must be responsible stewards of personal data and be accountable for their actions. Accountability requires organizations to be both responsible and answerable for any misuse of information.

(o) Accountability requires organizations to have policies that link to the law, mechanisms to put them in place, security safeguards, internal oversight, and documentation for basic processes.

(p) Data should be collected, created, used, and disclosed within the context of the relationship between the individual to whom the data pertains and the organization, based on the reasonable expectations of individuals as a group. It should be processed only for legitimate uses that have been disclosed or are in the context of those uses, and only the data necessary for those uses should be collected, created, used, or disclosed.

(q) Individuals expect to know about data uses that may have a significant impact on them and to be able to control those uses through an appropriate level of consent.

(r) Individuals should have the ability to question the use of data that impacts them and to challenge situations where use may create a negative impact.

(s) Individuals should be able to access data they provided to an organization, to understand what observational data is created by the organization, and to be told what types of data are inferred by analytical algorithms.

(t) The United States needs a new 21st century paradigm for regulating the use of personal data that incentivizes organizations to optimize beneficial uses of data while simultaneously minimizing adverse consequences for individuals and society as a whole. A national framework based on accountability and risk assessment, backed by robust oversight and enforcement, meets this objective. Moreover, an accountability framework will increase the confidence of individuals and organizations across the United States and beyond that their data will be protected wherever and by whomever it is stored or processed.

Section 1.03 DEFINITIONS.

(a) ADVERSE PROCESSING IMPACT.—The term "adverse processing impact" means detrimental, deleterious, or disadvantageous consequences to an individual arising from the processing of that individual's personal data or to society from the processing of personal data, including—

(1) direct or indirect financial loss or economic harm;

(2) physical harm;

(3) psychological harm, including anxiety, embarrassment, fear, and other mental trauma;

(4) inconvenience or expenditure of time;

(5) a negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to employment (including hiring, firing, promotion, demotion, reassignment, or compensation), credit and insurance (including denial of an application, obtaining less favorable terms, cancellation, or an unfavorable change in terms of coverage), housing, education, professional certification, issuance of a license, or the provision of health care and related services;

(6) stigmatization or reputational harm;

(7) disruption and intrusion from unwanted commercial communications or contacts;

(8) price discrimination;

(9) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing adverse processing impact, that materially—

(A) alter that individual's experiences;

(B) limit that individual's choices;

(C) influence that individual's responses; or

(D) predetermine results or outcomes for that individual.

(10) other detrimental or negative consequences that affect an individual's private life, including private family matters, actions, and communications within an

individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected, observed, or used; and

(11) with respect to detrimental, deleterious, or disadvantageous consequences to society arising from processing personal data, such other demonstrable consequences that may negatively impact a community or the public, taking into account factors such as national security, consumer confidence, the effective and efficient operation of government, effect on the public welfare, or ongoing or disproportionate allocation of risk on a particular population or community.

(b) AUTOMATED PROCESSING.—The term "automated processing" means processing through a machine-based system that can, for a given set of objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Automated processing—

(1) includes techniques such as machine learning, artificial intelligence, deep learning, analytics, or the use of algorithms—

(A) performed by or in computer software, physical hardware, or any other digital context; and

(B) designed to learn to approximate a cognitive task, solve complex problems, make predictions, adapt to changing circumstances, or improve performance when exposed to new or existing data sets.

(2) may operate with varying levels of autonomy or human intervention;

(3) may, but need not, involve human-like sensing, perception, cognition, reasoning, planning, learning, communication, decision-making, or physical action; and

(4) includes intelligent in-home assistants, computer vision systems, automated vehicles, unmanned aerial systems, voicemail transcription, advanced game-playing software, facial recognition systems, statistical models used to predict the probability of a particular future outcome, or other processing activity that involves automation of analysis and decision making.

(c) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(d) COVERED ENTITY.—

(1) The term "covered entity" means—

(A) any person subject to the authority of the Commission pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

(B) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); or

(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986; and

(D) such person, common carrier, or non-profit organization is or has engaged in processing personal data.

(2) Such term does not include—

(A) the Federal Government or any instrumentality of the Federal Government, nor the government of any State or political subdivision of any State; or

(B) an individual processing personal data—

(A) in the context of purely personal or household activities; or

(B) acting in a de minimis commercial capacity.

(e) IDENTIFIABLE INDIVIDUAL.—The term "identifiable individual" means an individual who can be identified, directly or indirectly, by an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

(f) INDIVIDUAL.—The term "individual" means a living natural person or an agent, trustee, or representative acting on behalf of a living natural person.

(g) INFERRED DATA.—The term "inferred data" means personal data created or derived through the analysis or interpretation of input information, features of data, and generalizations that is probabilistic in nature, often used for predictive purposes, classifying, profiling, personalization, customization, automated

decisions, risk or eligibility assessment, or other scoring. Inferred data may be created or derived through processing or automated processing.

(h) INFORMED CONSENT.—The term "informed consent" means a clear affirmative act establishing a freely given, specific, and unambiguous indication of the individual's agreement to the processing of personal data relating to the individual.

(i) OBSERVED DATA.—The term "observed data" means personal data captured by automatically recording the actions of an individual. Observed data includes data collected automatically by a covered entity, such as—

(1) static or video images collected from cameras;

(2) voice or other audible information collected from microphones;

(3) data regarding an individual's real-time location or location history over time collected through global positioning systems (GPS), a device's proximity to Wi-Fi hotspots, cell tower triangulation, or other similar automated method;

(4) information about an individual's movements, behavior, or health collected from connected device sensors, such as a gyroscope, accelerometer, magnetometer, proximity sensor, ambient light sensor, touchscreen sensor, pedometer, barometer, heart rate sensor, or thermometer; and

(5) data about an individual's browser history, mobile application use, online posts, comments or similar digital communications, social media use, or interactions with similar devices, platforms, or applications.

(j) PERSONAL DATA.—

(1) The term "personal data" means any information relating to an identified or identifiable individual, in any medium, including paper and electronic information.

(2) Such term does not include information about employees or employment status collected or used by an employer pursuant to an employer-employee relationship.

(k) PROCESSING.—The term "processing" means any operation or set of operations which is performed on personal data, such as collection, creation, recording, structuring, storage, analysis, adaptation or alteration, retrieval, consultation, use,

retention, disclosure, dissemination or otherwise making available, deletion, disposal, or destruction.

(l) PROCESSING ACTION.—The term "processing action" means a single, discrete processing operation performed on personal data, often characterized as one stage of the information lifecycle, including creation, collection, dissemination, duplication, transfer, use, retrieval, analysis, storage, disposition, de-identification, destruction, or deletion.

(m) PROCESSING ACTIVITY.—The term "processing activity" means a specific set of operations performed on personal data that defines the circumstances under which personal data are processed, including the business or other context; legal or regulatory requirements; boundaries of an information technology system; stages within the lifecycle of personal data; or the individual, covered entity, and other stakeholders directly or indirectly served or affected by the processing. A processing activity may be identified with reference to a specific system, product, service, technology, method of processing, business model, or business function, among other things, as determined by a covered entity pursuant to a documented policy.

(n) PROCESSING RISK.—

(1) The term "processing risk" means the level of adverse processing impact potentially created as a result of or caused by processing, a specific processing activity, or a specific processing action, assessed as a function of—

(A) the likelihood that adverse processing impact will occur as a result of processing, a specific processing activity, or a specific processing action; and

(B) the degree, magnitude, or potential severity of the adverse processing impact, should it occur.

(2) Processing risk shall be assessed and identified as one of five distinct levels:

(A) MINIMAL.—Processing that could reasonably be expected to create trivial, negligible, or de minimis adverse processing impact.

(B) LOW.—Processing that could reasonably be expected to create minor or limited adverse processing impact.

(C) MODERATE.—Processing that could reasonably be expected to create serious or significant adverse processing impact.

(D) HIGH.—Processing that could reasonably be expected to create severe or major adverse processing impact.

(E) EXTREME.—Processing that could reasonably be expected to create dire or catastrophic adverse processing impact.

(o) PROVIDED DATA.—

(1) The term "provided data" means personal data provided to a covered entity directly by the individual who is the subject of the personal data. Provided data includes personal data provided by the individual to the covered entity, such as—

(A) online or in-store transaction records, including credit or debit account information and contact information;

(B) account or event registration information;

(C) medical history given directly to a medical provider;

(D) password and answers to security questions entered to authenticate a user;

(E) response to a survey, questionnaire, contest, feedback form, comment field, or other inquiry or communication from the covered entity; or

(F) information submitted by an individual as part of an application process or inquiry.

(2) Such term does not include observed data, inferred data, or third-party provided data.

(p) SERVICE PROVIDER.—The term "service provider" means a person that—

(1) processes personal data on behalf of and at the sole direction of a covered entity;

(2) may not process such personal data except on instructions from the covered entity, unless otherwise required to do so by law; and

(3) may not disclose the personal data received from or on behalf of the covered entity, or any personal data derived from such personal data, other than as directed by the covered entity.

(q) SOCIETAL BENEFIT.—

(1) The term "societal benefit" means a material, objective, and identifiable positive effect or advantageous outcome accruing to the public as a result of the processing of personal data. To meet the requirements of this Act, a societal benefit must—

(A) promote and enhance the well being of the general public; and

(B) be separate and distinct from any positive outcome, advantageous impact, or value that accrues to a covered entity, single person or individual, or a narrow or specific group of persons.

(2) Examples of factors that may be considered include greater access to health care; better or lower cost health care; improvements to the general welfare; improvements to education; environmental enhancements, such as water conservation; energy cost reduction; protection of rights; and improved services or ease of use of services.

(r) THIRD PARTY.—The term "third party" means, with respect to any covered entity, a person that—

(1) is not a service provider; and

(2) is not related to the covered entity by common ownership or corporate control.

(s) THIRD-PARTY PROVIDED DATA.—The term "third-party provided data" means personal data provided to a covered entity from—

(1) an individual other than the individual who is the subject of the personal data;

(2) a third party;

(3) a government or any instrumentality of a government; or

(4) any other person.

Article II. FAIR PROCESSING OF PERSONAL DATA

Section 2.01 LAWFUL, RESPONSIBLE, AND FAIR PROCESSING.

(a) PERMISSIBLE PROCESSING.—A covered entity may process personal data when—

(1) the purpose of the processing is—

(A) for an identified legitimate use; or

(B) consistent with the context of the relationship between the individual and the covered entity.

(2) the processing is necessary and proportionate in relation to the purpose; and

(3) the covered entity has established, implemented, tested, revised, and documented reasonable and appropriate policies, procedures, and technical controls, taking into account the specific purpose of the processing and the level of processing risk.

(b) LEGITIMATE USE.—The use of an individual's personal data is legitimate for the purposes of this Act only when a covered entity can demonstrate one or more of the following:

(1) COMPLIANCE WITH LEGAL OBLIGATIONS.—The use is necessary to comply with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures required by court order, subpoena, summons, or other properly executed compulsory process.

(2) INFORMATION SECURITY.—The use is necessary to protect the security of devices, networks, or facilities against malicious, fraudulent, or illegal activity, or to prosecute those responsible for that activity.

(3) ONGOING BUSINESS PROCESSES.—The use is necessary to facilitate, improve, or safeguard the logistical or technical ability of the covered entity to provide goods or services to the individual, manage its operations, or protect against risk, including the use of personal data to—

(A) provide, operate, or improve a specific product or service used, requested, or authorized by the individual, including the ongoing provision of customer service and support;

(B) analyze the individual's use of a product or service provided by the covered entity to improve the covered entity's products, services, or operations; or

(C) support basic business functions that enable a covered entity to operate efficiently, such as accounting, billing, payment processing, inventory and supply chain management, warranty fulfillment, human resource management, quality assurance, and internal auditing.

(4) PROTECTION OF PROPERTY RIGHTS.—The use is necessary to protect or defend the covered entity's rights or property, including intellectual property, against actual or potential security threats, fraud, theft, unauthorized transactions, or other illegal activities.

(5) PUBLIC SAFETY AND HEALTH.—The use is necessary to protect the health or safety of the individual, a group of individuals, or larger community, taking into account the totality of the circumstances pertaining to a particular threat, including cooperation with law enforcement agencies concerning conduct or activity that the covered entity reasonably and in good faith believes may violate local, state, or federal law.

(6) INFORMED CONSENT.—

(A) Before a covered entity begins processing the personal data of an individual, the covered entity—

(i) obtains informed consent from the individual for the specific use; and

(ii) makes available to the individual a reasonable means to withdraw consent.

(B) A covered entity shall not be required to honor an individual's request to withdraw consent pursuant to one or more exceptions set forth in this Act, or as otherwise provided by law, if the covered entity identifies and clearly explains the limitations on withdrawing consent prior to obtaining informed consent.

(7) KNOWLEDGE DISCOVERY.—The personal data is used to extract insights, acquire knowledge, generate accurate predictions, detect patterns, identify anomalies, pursue truth, and avoid errors through research, investigation, and analysis. In order to rely upon knowledge discovery as the legitimate use for processing, a covered entity must—

(A) identify knowledge discovery as the purpose of the specific processing activity;

(B) be able to demonstrate that the specific knowledge discovery activity cannot reasonably be performed without personal data and that the personal data being processed is relevant and necessary for the particular processing;

(C) maintain on an ongoing basis a complete, accurate, and appropriately detailed inventory of specific knowledge discovery activities conducted across the covered entity;

(D) prohibit the use or application of the result or outcome of processing for knowledge discovery for any activities, measures, decisions, products, or services that may impact or relate to an individual or group of individuals, unless the covered entity can establish that the subsequent use or application of the knowledge discovered satisfies the requirements for a separate and independent legitimate use as otherwise required by this Section; and

(E) designate a qualified employee who shall—

(i) be responsible and accountable for the specific knowledge discovery processing activity; and

(ii) certify in writing on an annual basis that the covered entity is in compliance with the requirements of Section 2.01(b)(7) of this Act. Such certification shall be maintained by the covered entity and be available to demonstrate compliance with this Act.

(8) DEFINED AND DOCUMENTED BENEFITS.—After completing and documenting a processing impact assessment as required by Article V of this Act, the covered entity concludes with a reasonable degree of certainly certainty that—

1) the specific use of an individual's personal data, alone or in combination with other data, produces a material, objective, and identifiable benefit for the individual or society; and

2) the use of the individual's personal data—

(i) creates a minimal level of processing risk; or

(ii) creates no more than a moderate level of processing risk, and—

(I) the risk is necessary and proportional to the benefit;

(II) the risk has been mitigated to the extent practicable; and

(III) after all practicable controls to mitigate such risk have been identified and implemented, the material, objective, and identifiable benefit is not outweighed or counterbalanced by the residual level of processing risk.

(c) RESPECT FOR CONTEXT.—A covered entity may process an individual's personal data when the purpose of processing is consistent with the context of the relationship between the individual and the covered entity. Processing of personal data of an individual is consistent with the context of the relationship between the individual and the covered entity if such processing is within the reasonable expectation of similarly situated individuals.

(1) When assessing the reasonable expectation of similarly situated individuals, a covered entity shall consider, at a minimum—

(i) the specific use of the personal data, including whether the use would be obvious to an individual under the circumstances;

(ii) the sensitivity of the personal data, considered from the perspective of the individual and taking into account the full range of potential adverse consequences identified in Section 1.03(a) of this Act;

(iii) the level of processing risk associated with the specific processing activity;

(iv) the source of the personal data, including whether the personal data was collected directly from the individual;

(v) the method of collection;

(vi) for observed data, the extent to which an individual is likely to be aware of the observation occurring as a result of the presence of sensors or other devices, is likely to be aware that such sensors or devices are creating or processing observed data about the individual, or otherwise has knowledge of the processing;

(vii) the extent to which an individual engaged in one or more transactions directly with the covered entity, including whether the individual and covered entity maintain an ongoing commercial or other relationship;

(viii) the application of automated processing and transparency of such processing;

(ix) the accuracy and completeness of the personal data for the intended use; and

(x) the age and sophistication of similarly situated individuals who use the covered entity's products or services, including whether a product or service

is directed toward or significantly used by a vulnerable population identified in Section 5.02(b)(10) of this Act.

(2) Fraud prevention, authentication and identification, and information security shall be deemed to be consistent with the context of the relationship between the individual and the covered entity for the purposes of this Act.

(d) REASONABLE BASIS.—It is unlawful and an independent and separate violation of this Act for a covered entity to rely upon a specific legitimate use as set forth in Section 2.01(b) of this Act or claim that processing is consistent with the context of the relationship between the individual and the covered entity as set forth in Section 2.01(c) of this Act for the purpose of complying with Section 2.01(a) of this Act, without having a reasonable basis for such reliance or claim. The failure to conduct an investigation or analysis prior to processing shall be evidence that a covered entity did not have a reasonable basis.

Section 2.02 RESTRICTIONS ON PROCESSING.

(a) EXTREME RISK.—Notwithstanding Section 2.01, a covered entity shall not process personal data when the processing is reasonably likely to produce an extreme level of processing risk unless, at a minimum—

(1) the processing is expressly authorized by statute; and

(2) the covered entity is in compliance with the applicable requirements of this Act.

(b) NO UNDISCLOSED PROCESSING.—A covered entity shall not process an individual's personal data unless the covered entity makes available to the individual and the public the information required in Section 3.01 of this Act.

(c) EXCEPTIONS TO SECTIONS 2.01(b)(8) AND 2.01(c).—Notwithstanding Section 2.01 above, a covered entity may not rely on defined and documented benefits as a legitimate use for processing or respect for context if such processing is likely to create a high or extreme level of processing risk.

(d) PROCESSING IN ABSENCE OF FAIR MUTUAL BENEFIT.—

(1) BENEFIT OF PROCESSING:

(A) An individual should receive a material, objective, and identifiable benefit, directly or indirectly, from the processing activities of a covered entity when the covered entity processes the personal data of the individual.

(B) An individual may be the direct recipient of a benefit or may indirectly derive value from the benefit. A benefit in this context may include personalized services, the provision of a product or service at no or reduced cost, the provision of more efficient services, discounts related to loyalty programs, increased accuracy of data retrieval, or other value.

(C) A benefit for the purpose of this paragraph may not be purely speculative, presumed to exist or presumed to produce a positive impact.

(D) A rebuttable presumption exists that a societal benefit is considered a benefit to the individual for the purpose of this Section.

(2) PROHIBITION ON PROCESSING IN ABSENCE OF BENEFIT.—Notwithstanding Section 2.01 of this Act—

(A) A covered entity may not process an individual's personal data if a covered entity exclusively or disproportionately derives the benefit from the processing such that any benefit that enures to the individual is grossly inequitable, cannot be assessed or identified with any degree of specificity, or is manifestly unreasonable under the circumstances.

(B) EXCEPTION.—Notwithstanding subparagraph (A) above, a covered entity may process an individual's personal data if the covered entity concludes with a reasonable degree of certainty, after conducting a processing impact assessment as set forth in Article V of this Act, that the processing of the individual's personal data creates a minimal level of processing risk.

Section 2.03 UNETHICAL AND RECKLESS PROCESSING.—Regardless of the legitimate use or permissible basis for processing, when processing the personal data of an individual a covered entity has a legal duty to that individual to take measures to prevent reasonably foreseeable adverse processing impact to that individual. A covered entity violates this legal duty and this Act when the covered entity acts with reckless disregard for processing risk or for adverse processing impact to the individual.

(a) When determining if a covered entity engaged in processing with such reckless disregard in a given context in violation of this Act, the following factors shall be considered—

(1) the covered entity's intent to undertake the processing that created the processing risk or caused the adverse processing impact to the individual;
(2) the foreseeability of the processing risk or the adverse processing impact to the individual;
(3) the closeness or proximity of the connection between the processing and the severity of adverse processing impact suffered by the individual; and
(4) the extent to which the measures that could have been taken to mitigate processing risk were reasonably available or considered industry best practice at the time of the processing.

(b) A covered entity may act with reckless disregard and thereby violate its legal duty to an individual and this Act even if the covered entity does not intend to cause adverse processing impact. For the purposes of this Act, it is sufficient to establish that the covered entity intended to undertake the processing that caused the adverse processing impact to the individual.

(c) A violation of Section 2.03 of this Act shall constitute a separate and independent violation of this Act.

Article III. RESPONSIBILITIES OF ACCOUNTABLE COVERED ENTITIES

Section 3.01 OPEN AND TRANSPARENT PROCESSING.

(a) COMPREHENSIVE PUBLIC STATEMENT OF POLICIES AND PRACTICES.—A covered entity shall publish and make readily available to the public on an ongoing basis a comprehensive statement about the covered entity's processing and an individual's options with regard to such processing, including the following information—

(1) the identity of the covered entity, including any relevant affiliates, subsidiaries, or brands necessary to convey meaningful information to an individual;
(2) the covered entity's guiding principles for accountability and data responsibility as required by Section 4.01(b) of this Act;
(3) a description of the categories of provided data, third-party provided data, observed data, and inferred data processed by the covered entity;

(4) for each category of personal data identified pursuant to paragraph (a)(3) above, a description of the use of the personal data and purpose for processing, unless the processing is reasonably likely to create a high or greater level of processing risk, in which case the covered entity shall provide a clear and detailed explanation of the specific use of the personal data and purpose for processing;

(5) information regarding automated processing as required by Section 3.01(d) of this Act;

(6) the specific purposes for which personal data may be disclosed or transferred to a third party and the categories of third parties who may receive such personal data;

(7) an explanation of how an individual may exercise each option available to the individual with respect to the processing of the individual's personal data as required by Sections 3.02, 3.04, 3.05, and 3.06 and Article VI of this Act;

(8) any material changes to the covered entity's processing practices implemented in the preceding 12 months; and

(9) the effective date of the statement.

(b) MEANINGFUL SUMMARY EXPLANATION OF PROCESSING DIRECTED TO THE INDIVIDUAL.—A covered entity shall publish and make readily available to the public on an ongoing basis a summary of the covered entity's processing practices and activities. Such statement shall—

(1) be drafted in a concise, intelligible, and easily accessible form, using clear and plain language;

(2) identify the covered entity, including any relevant affiliates, subsidiaries, or brands necessary to convey meaningful information to an individual;

(3) provide an individual with a meaningful overview of the processing of the individual's personal data;

(4) provide an individual with a meaningful overview of the individual's options with respect to the processing of the individual's personal data as required by Sections 3.02, 3.04, 3.05, and 3.06 and Article VI of this Act;

(5) enable an individual to make a reasonably informed decision regarding the processing of the individual's personal data and the options available to the individual; and

(6) link to the statement required in Subsection (a).

(c) ADDITIONAL TRANSPARANCY AND ACCOUNTABILITY FOR HIGH RISK PROCESSING.—

(1) EXPLICIT NOTICE.—A covered entity shall provide explicit notice to an individual prior to the collection from that individual of personal data that is reasonably likely to create a high or greater level of processing risk.

(2) ENHANCED DISCLOSURES.—A covered entity shall conduct and document an analysis to determine if additional methods of notice and communication are necessary to provide an individual with clear, meaningful, relevant, and timely information regarding the covered entity's processing practices in a given context or circumstance. In conducting this analysis, a covered entity shall consider how an individual may obtain such information and assert their preferences, including the extent to which an individual has an opportunity to interact directly with information presented on a computer or mobile screen or similar mechanisms to configure preferences or exercise control over the way in which their personal data is processed. Such analysis shall be incorporated in the processing impact assessment required by Section 5.04 of this Act and be conducted when—

(A) the covered entity launches a new processing activity or makes material modifications to a current processing activity; and

(B) the new or modified processing activity creates a high or greater level of processing risk.

(d) TRANSPARENCY AND EXPLAINAIBLITY FOR AUTOMATED PROCESSING.—

(1) A covered entity shall establish one or more mechanisms to inform an individual when automated processing is used to make a decision about the individual or that may affect the individual and the potential implications of such decision.

(2) The mechanism for providing the required information shall take into account the specific context of the processing and shall, to the extent practicable, provide the individual with notice at the point of interaction.

(3) The notice shall, at a minimum, be designed to—

(A) make an individual aware of the individual's interaction with automated processing;

(B) enable an individual to understand the purpose of the automated processing and the outcome; and

(C) enable an individual adversely affected by automated processing to challenge the outcome based on plain and easy-to-understand information on the factors and the logic that served as the basis for the prediction, recommendation, decision, or other outcome.

Section 3.02 MEANINGFUL CONTROL.

(a) OPT OUT.—A covered entity shall make available a means for an individual to opt out of the use of the individual's personal data.

(b) HIGH RISK PROCESSING.—A covered entity should, where practicable, obtain informed consent from an individual before a covered entity processes that individual's personal data if the processing is reasonably likely to create a high level of processing risk.

(c) EXTREME RISK.—Unless otherwise provided by law, a covered entity shall obtain informed consent from an individual before a covered entity processes that individual's personal data where the processing is reasonably likely to create an extreme level of processing risk.

(d) WITHDRAWAL OF CONSENT.—A covered entity shall provide an individual with a means to withdraw consent granted under this Section and Section 2.01(b)(6) of this Act.

(e) DISCONTINUE THIRD-PARTY TRANSFERS.—A covered entity shall provide an individual with a means to request that the covered entity stop sharing, selling, licensing, transferring, providing, or otherwise make available the individual's personal data to third parties.

Section 3.03 DATA QUALITY, ACCURACY, AND RETENTION.

(a) A covered entity shall ensure that personal data processed by the covered entity is reasonably accurate, complete, and current. In determining whether personal data is reasonably accurate, complete, and current in a given context, a covered entity shall consider, at a minimum—

(1) the legitimate use of the personal data; and

(2) the level of processing risk.

(b) A covered entity shall not maintain personal data in identifiable form once the personal data is no longer necessary for a legitimate use.

Section 3.04 ACCESS.

(a) ACCESS TO PERSONAL DATA.—Upon receiving a verified request from an individual, a covered entity shall provide the individual with confirmation as to whether or not the covered entity is processing personal data about the individual and, when the response is in the affirmative, shall provide the individual with reasonable access to the individual's personal data retained by the covered entity as follows:

(1) Provided data.

(2) Third-party provided data, including information as to the source of the personal data, where practicable.

(3) With respect to observed data—

(A) a list of the specific categories of data that have been observed about the individual;

(B) the specific purpose and legitimate use for processing each of the specific categories of observed data; and

(C) confirmation that a processing impact assessment was conducted pursuant to Article V of this Act and the level of processing risk assigned to the observed data or relevant processing activity.

(4) With respect to inferred data—

(A) a list of the specific categories of data that have been inferred about the individual;

(B) the specific purpose and legitimate use for processing each of the specific categories of inferred data;

(C) the reasonably anticipated consequences of such processing and the level of processing risk assigned to the inferred data or relevant processing activity; and

(D) where the processing of the inferred data creates a moderate or greater level of processing risk, meaningful information about the process or methodology employed to create the inferred data.

(b) STATEMENT OF ACCOUNTABILITY IN LIEU OF ACCESS.—

(1) Where a covered entity can demonstrate that it is unduly burdensome, technically infeasible, and not practicable to provide an individual with access to all or a subset of the individual's personal data as otherwise required by this Act, and has determined with a high degree of certainty that the processing does not create a high or greater level of processing risk, a covered entity may provide an individual with a written statement explaining the reasons that access cannot be provided and confirming that the processing of the individual's personal data is subject to internal policies, procedures, and other controls for the processing of personal data necessary to ensure lawful, responsible, and accountable processing given the intended uses of the data and the level of processing risk.

(2) It shall be unlawful and a separate violation of this Act for a covered entity to rely upon Section 3.04(b) of this Act in bad faith or provide a statement as required in Section 3.04(b) of this Act that is false, misleading, or inaccurate.

(c) ACCESS TO INFORMATION ABOUT SHARING WITH THIRD PARTIES.—Upon receiving a verified request from an individual, a covered entity shall provide the individual with a list identifying the specific category or categories of third parties with whom the covered entity shares the individual's personal data, unless the processing is reasonably likely to create a high or greater level of processing risk, in which case the covered entity shall provide the individual with a list identifying the specific third parties with whom the covered entity shares or has shared the individual's personal data and the purpose for such sharing.

(d) BUSINESS CONTINUITY PLAN.—A covered entity shall identify those circumstances in which the inability of an individual to access the individual's personal data is reasonably likely to create a high or greater level of processing risk. Where such processing risk exists, a covered entity shall develop, document, and implement an appropriate business continuity plan in order to ensure services and access can be reasonably maintained and restored as appropriate.

Section 3.05 DATA PORTABILITY.

(a) PROVIDED DATA.—Upon receiving a verified request from an individual, a covered entity shall, where technically feasible, make available a reasonable means for an individual to transmit or transfer provided data and third-party provided data about the individual retained by the covered entity to another covered entity in a structured, standardized, and machine-readable interoperable format, or otherwise download personal data for the individual's own use.

(b) OBSERVED AND INFERRED DATA.—A covered entity may decline to provide an individual with the ability to transfer, transmit, or download personal data as specified in Section 3.05(a) for observed or inferred data if the transfer, transmission, or download of such data could—

(1) reasonably be expected to reveal confidential, proprietary or trade secret information, or other intellectual property; or

(2) provide a competitor with the benefit or value of processing undertaken by the covered entity to the disadvantage of the covered entity.

Section 3.06 RESPONSIBLE AND ACCESSIBLE REDRESS.

(a) CORRECTION OF PERSONAL DATA.—A covered entity shall make available a mechanism for an individual to dispute and resolve the accuracy or completeness of personal data.

(b) DELETION OF PERSONAL DATA.—A covered entity shall make available a mechanism for an individual to obtain deletion, to the extent practicable, of personal data. In response to a request to delete personal data, the covered entity shall, to the extent practicable, delete such data from its records and direct any service providers to delete the individual's personal data from their records.

(c) CHALLENGE AUTOMATED PROCESSING.—A covered entity shall make available a mechanism for an individual to challenge the outcome of automated processing when the individual has reason to believe that the individual suffered adverse processing impact as a result of the prediction, recommendation, decision, or other outcome of the automated processing.

(d) COMPLAINT PROCESS.—A covered entity shall provide an individual with a mechanism to submit a complaint or inquiry regarding a covered entity's policies and procedures relating to the processing of the individual's personal data or compliance with this Act.

(e) ADDITIONAL REDRESS MECHANISMS FOR HIGH RISK PROCESSSING.—A covered entity with more than 500 employees and annual revenue in excess of $25 million shall conduct and document an analysis before commencing any processing activity that creates a high or greater level of processing risk in order to determine if additional or special redress mechanisms are warranted given the nature and scope of the covered entity's activities and data holdings. Such analysis shall be incorporated in the processing impact assessment required by Article V of this Act.

Section 3.07 INFORMATION SECURITY.

(a) A covered entity shall develop, implement, and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards to protect the security, confidentiality, integrity, and availability of personal data. Such program shall be appropriate to the covered entity's size and complexity, the nature and scope of the covered entity's activities, and the sensitivity of personal data processed by the covered entity.

(b) In order to develop, implement, and maintain an information security program, a covered entity shall—

(1) identify reasonably foreseeable internal and external risks to the confidentiality, integrity, and availability of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such data, and assess the sufficiency of any safeguards in place to control these risks;

(2) maintain ongoing awareness of information security, vulnerabilities, threats, and incidents;

(3) develop and implement incident management policies and procedures that address incident detection, response, and recovery;

(4) design and implement safeguards to control reasonably foreseeable risks through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; and

(5) evaluate and adjust the covered entity's information security program in light of the results of the testing and monitoring, material changes to operations or business arrangements, or other circumstances that may have a material impact on the covered entity's information security program.

Section 3.08 PROCEDURES, EXCEPTIONS, AND RULE OF CONSTRUCTION.

(a) REASONABLE PROCEDURES.—

(1) A covered entity shall make available a reasonably accessible, conspicuous, and easy-to-use means for an individual to exercise each option required by Article III of this Act.

(2) An individual shall be entitled to submit a complaint or inquiry as required by Section 3.06(d) of this Act and exercise each option required by Sections 3.02(a), 3.02(d), and 3.02(e) of this Act at any time and at no cost to the individual.

(3) An individual shall be entitled to exercise each option required by Sections 3.04, 3.05, 3.06(a), and 3.06(b) of this Act, at no cost to the individual, once in a 12-month period with respect to a processing activity.

(4) An individual shall be entitled to exercise the option required by Section 3.06(c) of this Act, at no cost to the individual, once in a 12-month period for each automated processing activity.

(5) A covered entity shall honor an individual's request pursuant to Sections 3.02(a) and 3.02(d) of this Act without undue delay and no later than 7 business days following the request.

(6) With respect to a request or complaint filed by an individual pursuant to Sections 3.02(e) 3.04, 3.05, 3.06(a), 3.06(b), 3.06(c) and 3.06(d) of this Act, a

covered entity shall respond to the individual without undue delay and no later than 30 days after receiving the request or complaint. The covered entity shall provide the individual with sufficient information to understand and act upon the response.

(b) EXCEPTIONS.—

(1) A covered entity shall not be required to comply with a request from an individual pursuant to Sections 3.02(a), 3.02(e), or 3.06(b) of this Act where the personal data or processing is necessary for the legitimate uses set forth in Sections 2.01(b)(1), 2.01(b)(2), 2.01(b)(4), or 2.01(b)(5) of this Act.

(2) A covered entity shall not be required to make available to an individual personal data pursuant to Sections 3.04 or 3.05 of this Act if—

(A) the personal data—

(i) was previously deleted by the covered entity in compliance with documented data retention schedules;

(ii) constitutes confidential commercial information, including an algorithm used to make predictions, inferences, scores, or other decisions; or

(iii) such access is limited by law, legally recognized privilege, or other legal obligation.

(B) a covered entity makes an individualized determination that fulfilling the request from the individual would create processing risk or legitimate risk to the security, safety, free expression, or other rights of another individual.

(3) A covered entity shall not be required to comply with Sections 3.01(d), 3.04(a)(3), 3.04(a)(4), 3.05, 3.06(a), 3.06(b), and 3.06(c) of this Act if the covered entity determines with a reasonable degree of certainty, after completing and documenting a processing impact assessment pursuant to Article V of this Act, that the processing will create no more than a low level of processing risk.

(4) A covered entity shall not be required to comply with a request from an individual or to respond to an individual's complaint or inquiry if the covered entity has reason to believe and can demonstrate that such request, complaint, or inquiry is frivolous, vexatious, and in bad faith.

(c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to require a covered entity to—

(1) take an action that would convert information that is not personal data into personal data; or

(2) delete, destroy, or de-identify data that is retained for backup or archival purposes to the extent that such systems are not and cannot be accessed in the ordinary course.

(d) RULEMAKING.—The Commission shall, within 1 year of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations to modify or add additional exceptions and limitations to the requirements set forth in Article III consistent with the purposes of this Act.

Article IV. ACCOUNTABLE PROCESSING

Section 4.01 ACCOUNTABLE PROCESSING MANAGEMENT PROGRAM.

(a) PURPOSE.—A covered entity shall establish, implement, maintain, and continually improve an accountable processing management program to—

(1) ensure compliance with this Act, other applicable legal or regulatory requirements, and industry best practices;

(2) promote effective management and oversight of processing across the covered entity;

(3) manage risk, including processing risk, on an ongoing basis;

(4) evaluate both adverse and beneficial impacts of processing on all relevant parties and consider the interests of such parties when making determinations about processing; and

(5) demonstrate the covered entity's ongoing commitment to trustworthy, fair, responsible, and transparent processing.

(b) GUIDING PRINCIPLES FOR ACCOUNTABILITY AND DATA RESPONSIBILITY.—

(1) ESTABLISH STRATEGIC VISION.—A covered entity shall define, document, and publish guiding principles regarding processing that identify, at a minimum, a covered entity's top-level goals and objectives, values, and strategic vision with respect to data stewardship, data ethics, responsible processing, and

accountability. The guiding principles should extend beyond meeting minimum regulatory requirements.

(2) SENIOR MANAGEMENT REVIEW AND APPROVAL.—The Board of Directors or equivalent senior governing body of a covered entity shall review and approve the guiding principles on an annual basis and require all processing across the covered entity to align with the covered entity's guiding principles for accountability and data responsibility.

(c) PROGRAM DEVELOPMENT AND IMPLEMENTATION.—A covered entity shall ensure that its accountable processing management program includes, at a minimum—

(1) a qualified senior executive to oversee the development, implementation, maintenance, and monitoring of the program;

(2) strategic planning that considers across the covered entity both personal data itself and the related resources, such as personnel, equipment, funds, and information technology;

(3) mechanisms to ensure ongoing collaboration between designated senior executives across different functions to ensure coordination of risk management, business operations, legal and regulatory compliance, security, and processing activities;

(4) documentation to demonstrate that a covered entity has an accountable processing management program in place and the capacity to comply with legal and program requirements on an ongoing basis. Such documentation shall provide an overview of the program, including a description of the—

(A) management and structure of the program;

(B) resources dedicated to the program;

(C) role of designated accountable officials and staff; and

(D) strategic goals and objectives of the program.

(5) resources, staff, policies, and procedures that are appropriate to—

(A) a covered entity's size and complexity;

(B) the nature and scope of a covered entity's activities;

(C) legal requirements and obligations that apply to such activities;

(D) the scale of a covered entity's processing operations; and

(E) the sensitivity of personal data processed and the level of processing risk created by the covered entity's processing activities.

(d) RESPONSIBLE DATA GOVERNANCE.—As part of an accountable processing management program, a covered entity shall—

(1) ensure that personal data is properly managed throughout its lifecycle, including all stages of processing, such as creation, collection, use, analysis, storage, maintenance, dissemination, disclosure, and disposition;

(2) establish policies and procedures to ensure that personal data is managed and maintained according to applicable laws, industry codes of conduct, industry best practices, and internal policies and procedures;

(3) be able to identify, distinguish, and appropriately manage different categories of personal data and personal data obtained, collected, received, or created from different sources, including provided data, third-party provided data, observed data, and inferred data;

(4) ensure that each processing activity has a designated accountable employee who can reliably describe how personal data is processed throughout the processing activity; and

(5) maintain a current, complete, and accurate inventory of the covered entity's information systems and information holdings, including the covered entity's information systems that process personal data.

Section 4.02 ETHICAL, TRUSTWORTHY, AND PREVENTATIVE DESIGN.

(a) PROGRAM OBJECTIVES.—When developing a new processing activity or updating an existing processing activity, a covered entity shall consider, evaluate, and integrate, as appropriate, technical and nontechnical processes, engineering analyses, design principles, and controls in order to build and deliver a more trustworthy processing activity and minimize adverse effects, including processing risk.

(b) PLANNING FOR TRUSTWORTHY DESIGN.—A covered entity shall, during the initial stages of any development process and throughout the various stages of the processing activity development lifecycle—

(1) inventory, incorporate, and apply the legal rules, industry best practices, contractual obligations, and internal requirements for the processing of personal data, anticipating and facilitating implementation of controls that may be necessary to support compliance;
(2) identify discrete processing actions within a given processing activity, and determine which data processing actions may create processing risk and assess the level of processing risk;
(3) establish and document a decision-making process that covers the life of each processing activity and includes explicit criteria for analyzing the benefits and risks, including information security and processing risk, associated with each stage in the lifecycle of both personal data and supporting technologies; and
(4) consider and document the impact of decisions and actions in each stage of the lifecycle.

(c) ASSESS AND IMPLEMENT REQUIREMENTS.—For each processing activity, a covered entity should—

(1) determine the need or desirability for the covered entity to have the capability to review, identify, access, transfer, segregate, tag, track, retrieve, alter, delete, and otherwise manage personal data;
(2) ensure that the required or desired capabilities are integrated into the design to the extent practicable;
(3) ensure that personal data can be managed or administered with sufficient granularity in order to provide confidence that inaccurate personal data can be identified and corrected, obsolete personal data is disposed of, personal data is processed only for legitimate uses, and that an individual's preferences about use and sharing of their personal data are implemented and maintained;
(4) conduct technical, process, and risk analyses of alternative design implementations in order to reduce risk and increase accountability;
(5) consider how a given system can be audited such that it is possible to trace any access to the information system, modifications made, and any action carried out, in order to identify its author; and

(6) avoid the use of personal data for testing processing activities to the extent feasible and implement controls to mitigate processing risk if personal data must be used.

Section 4.03 ACCOUNTABILITY FOR AUTOMATED PROCESSING.

(a) GENERAL OBLIGATIONS FOR TRUSTWORTHY AND ACCOUNTABLE AUTOMATED PROCESSING.—A covered entity engaged in automated processing shall—

(1) understand the reasoning behind any decision or recommendation produced by automated processing;

(2) exercise judgment in deciding whether to accept the decision or recommendation from automated processing;

(3) implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context of the specific automated processing and consistent with the state of art; and

(4) ensure overall fairness of making predictions about an individual from group-level data in a given context.

(b) SPECIFIC REQUIREMENTS FOR TRUSTWORTHY AND ACCOUNTBLE AUTOMATED PROCESSING.—A covered entity engaged in automated processing shall implement policies and procedures to ensure that—

(1) personal data used in or for automated processing is labeled or traceable to enable analysis of the outcome or decision from such automated processing and responses to an inquiry, appropriate to the context, including the level of processing risk and consistent with the state of art;

(2) reports including predictions include error bars, confidence intervals, or other similar indications of reliability to assist decision makers with giving the prediction appropriate weight;

(3) automated processing tools are designed and built to mitigate bias at both the model and data layers, and that proper protocols are in place to promote transparency and accountability. Such protocols shall address, as appropriate—

(A) the validity of the outcome, taking into account the context around how the personal data was collected and what kind of inference is being drawn;

(B) accuracy of the outcome, taking into account the automated processing model's performance; and

(C) bias of the outcome, including examination of potential bias at different stages of automated processing, imperfect data quality, missing data, sampling bias, or other relevant factors.

Section 4.04 ACCOUNTABILIY FOR PROCESSING BY SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—When a covered entity engages a service provider to process personal data, the covered entity shall—

(1) exercise appropriate due diligence in the selection of the service provider and take reasonable steps to maintain appropriate controls for the processing and security of the personal data;

(2) require the service provider by contract to implement and maintain appropriate measures designed to meet the objectives and requirements of this Act;

(3) prohibit the service provider by contract from processing the personal data for any purpose other than the specific purposes and legitimate uses for which the covered entity shared such personal data with the service provider;

(4) require, as appropriate, managers and staff of the service provider to complete education, awareness, and training programs related to processing; and

(5) exercise reasonable oversight and take reasonable actions to ensure compliance with such contractual provisions, including the implementation of an assessment process to periodically determine whether the service provider has reasonable and appropriate procedures in place to comply with this Act. The assessment process shall reflect the particular circumstances of the covered entity, including its size and complexity, the nature and scope of the covered entity's data holdings and activities with respect to personal data, and the relative level of processing risk.

(b) THIRD PARTIES.—A covered entity shall not sell, license, or otherwise transfer personal data it holds to a third party, unless that third party is contractually bound to meet the same processing and security obligations as the covered entity under this Act and any additional obligations to which the covered entity has

publicly committed. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure a third party's compliance with such contractual provisions.

(c) ASSITANCE OR SUPPORT FOR VIOLATING THIS ACT.—It shall be unlawful and a separate violation of this Act for a covered entity to provide substantial assistance or support for or related to the processing of personal data to any person when that covered entity knows or consciously avoids knowing that the person is engaged in ongoing or systemic acts or practices that violate this Act. Nothing in this Section shall prohibit a covered entity from providing assistance or support to a person for the sole purpose of coming into compliance with the provisions of this Act.

Section 4.05 EMPLOYEE ACCOUNTABILITY.

(a) DESIGNATION OF REPONSIBLE AND ACCOUNTABLE EMPLOYEES.—A covered entity shall designate one or more qualified employees who have organization-wide responsibility and accountability for developing, implementing, and maintaining policies and procedures to ensure compliance with this Act.

(b) AWARENESS AND TRAINING PROGRAMS.—A covered entity shall develop, maintain, and implement an appropriate education, awareness, and training program for all employees. As part of such program, a covered entity shall provide—

(1) foundational as well as more advanced levels of training;

(2) role-based training to employees with assigned roles and responsibilities with respect to the processing of personal data and compliance with this Act; and

(3) training and awareness for employees specifically on how to report and respond to incidents that may affect the confidentiality, availability, or integrity of personal data.

(c) NEEDS ASSESSMENT.—A covered entity shall establish policies and procedures to assess and address the hiring, training, continuing education, and professional development needs of employees with roles and responsibilities related to compliance with this Act.

(d) INTERNAL ENFORCEMENT.—A covered entity shall document and implement policies and procedures to ensure that all employees are held accountable for complying with organization-wide information security and personal data processing requirements and policies, including procedures for internal enforcement of the covered entity's policies and discipline for non-compliance.

Section 4.06 OVERSIGHT: DEMONSTRATING TRUSTWORTHINESS, COMPLIANCE, AND ONGOING COMMITMENT TO RESPONSIBLE PROCESSING.

(a) INTERNAL REVIEWS.—A covered entity shall establish an independent and objective internal review, audit, and assurance program to—

(1) monitor compliance with legal obligations, including statutory, regulatory, and contractual obligations;

(2) monitor compliance with internal policies and procedures and alignment with public representations;

(3) confirm that the covered entity's processing activities are conducted as planned;

(4) evaluate the effectiveness of the covered entity's compliance with this Act; and

(5) assess whether risk assessments required by Article V of this Act have been conducted with integrity and competency.

(b) POTENTIAL CONFLICTS OF INTEREST.—A covered entity shall implement reasonable and appropriate procedures to ensure that—

(1) there is a clear separation of duties between different roles with respect to processing;

(2) an accountable official responsible for approving a processing impact assessment or approving a specific processing activity shall not have a private, personal, professional, financial, or other interest sufficient to appear to influence the objective exercise of his or her official duties; and

(3) the oversight process is independent from the assessment process.

(c) HIGH RISK PROCESSING ACTIVITY.—

(1) A covered entity shall create an internal data processing review board to evaluate and approve new processing activities, including automated processing, that creates a high or extreme level of processing risk and assess whether the

processing has been conducted with integrity and in full compliance with this Act; and

(2) A covered entity shall seek external review and validation, including external audits and certifications of policies, procedures, and practices to ensure compliance with relevant laws, industry best practices, internal procedures, and the requirements of this Act.

(d) EVIDENCE OF OVERSIGHT.—A covered entity shall document the oversight process in order to demonstrate how the oversight was conducted and that, in fact, it was conducted.

Article V. PROCESSING RISK MANAGEMENT

Section 5.01 RISK MANAGEMENT PROGRAM.

(a) PROGRAM OVERVIEW.—A covered entity shall establish, implement, maintain, and continually improve a program to manage reasonably foreseeable processing risk. The program shall include processes and procedures to—

(1) identify processing risk;

(2) assess the level of processing risk;

(3) mitigate processing risk;

(4) document residual processing risk;

(5) make an informed determination to accept residual processing risk and authorize processing; and

(6) monitor processing risk and that the controls put in place to mitigate processing risk over time to ensure that controls are—

(A) implemented correctly;

(B) operating as intended; and

(C) sufficient to ensure ongoing compliance with applicable requirements and to manage identified and evolving processing risk on a continual basis.

(b) Risk management shall be conducted as an entity-wide activity to ensure that risk-based decision-making is integrated into each aspect of the covered entity's planning and operations related to processing.

(c) A covered entity's risk management strategy shall include strategic-level decisions by senior leaders and executives regarding the management of risk, including the identification of risk assumptions, risk tolerance, priorities, and trade-offs.

Section 5.02 ASSESSMENT OF PROCESSING RISK.

(a) PROCESSING RISK.—When assessing the level of processing risk for a specific processing activity or processing action, a covered entity shall take into account—

(1) the likelihood that adverse processing impact will occur as a result of processing, a specific processing activity, or a specific processing action; and

(2) the degree, magnitude, or potential severity of the adverse processing impact, should it occur.

(b) CONSIDERATION OF CONTEXT.—To assess the potential severity and likelihood of adverse processing impact, a covered entity shall consider the context of processing and evaluate, at a minimum, the following factors:

(1) USE.—The specific purpose for which personal data is processed.

(2) SENSITIVITY OF PERSONAL DATA.—The sensitivity of specific data elements processed, as well as the sensitivity of the personal data, when combined with other data elements, considered from the perspective of the individual and taking into account the full range of potential negative consequences identified in Section 1.03(a) of this Act.

(3) REASONABLE EXPECTATIONS.—The extent to which an individual would reasonably expect the processing to occur.

(4) IDENTIFIABLITY AND LINKABILITY.—The extent to which a given data set is linked or linkable to an identifiable individual or an individual who can be identified from a given data set.

(5) IMPACT ON AN INDIVIDUAL.—Whether or not the result or outcome of processing is linked or linkable to an individual, the extent to which processing may negatively impact an individual.

(6) DATA SOURCES.—The sources and categories of personal data processed, including provided data, third-party provided data, observed data, and inferred data, taking into account the number of different and distinct sources of personal

data, such as devices, communication channels, accounts, online transactions, and offline transactions.

(7) DATA CREATION.—The extent to which a specific processing activity creates new personal data about an individual, including inferences, scores, or predictions.

(8) EXTENT OF SHARING AND TRANSER.—The extent to which personal data will be shared, sold, licensed, transferred, or otherwise provided to one or more third parties.

(9) DISCLOSURE.—Intended public disclosure of personal data or widespread dissemination.

(10) VULNERABLE POPULATIONS.—The extent to which the processing targets or otherwise involves a potentially vulnerable population, such as children, the elderly, individuals with a serious health condition or disability, victims of certain crimes, deployed members of the military and their families, communities recovering from crisis or disaster, or groups facing undue economic hardship.

(11) MITIGATION POTENTIAL.—The extent to which an individual would be able to discover, mitigate, and fully resolve any adverse processing impact caused by processing, taking into account the resources that would be required for an individual to resolve any adverse processing impact and obtain full redress.

(12) PERMANENCE.—The relevance and utility of personal data or the outcome of processing over time, including whether the personal data is immutable.

(13) DURATION.—The duration or frequency of the processing activity, ranging from a one-time use or single transaction to systemic, ongoing processing.

(14) AUTOMATED DECISIONS.—The extent to which data-enabled decisions are being made without human intervention.

(15) LEGAL OBLIGATIONS.—All statutory, regulatory, contractual, and other legal obligations or restrictions that may apply to the processing.

(16) SOCIETAL RISK.—Such other factors as may be relevant to a community or the public in a given set of circumstances.

Section 5.03 CATEGORIZATION OF PROCESSING RISK.

(a) LEVELS OF RISK.—When conducting a processing impact assessment as required by Sections 5.04 and 5.05 of this Act, a covered entity shall categorize the level of processing risk as one of the following:

(1) MINIMAL.—Processing that could reasonably be expected to create trivial, negligible, or de minimis adverse processing impact.

(2) LOW.—Processing that could reasonably be expected to create minor or limited adverse processing impact.

(3) MODERATE.—Processing that could reasonably be expected to create serious or significant adverse processing impact.

(4) HIGH.—Processing that could reasonably be expected to create severe or major adverse processing impact.

(5) EXTREME.—Processing that could reasonably be expected to create dire or catastrophic adverse processing impact.

(b) ILLUSTRATIVE REBUTTABLE PRESUMPTIONS TO INFORM RISK CATAGORIZATION.—

(1) MINIMAL.—The risk categorization level shall be presumed to be minimal if the processing—

(A) only involves provided data;

(B) does not include any categories of personal data identified in Sections 5.03(b)(3) or 5.03(b)(4) of this Act;

(C) is consistent with the context of the relationship between the individual and the covered entity; and

(D) does not involve the sharing or disclosure of personal data with third parties unless required for the legitimate uses set forth in Sections 2.01(b)(1) or 2.01(b)(5) of this Act.

(2) LOW.—The risk categorization level shall be presumed to be low if—

(A) processing is consistent with the context of the relationship between the individual and the covered entity;

(B) does not include any categories of personal data identified in Sections 5.03(b)(3) or 5.03(b)(4) of this Act;

(C) automated processing is not employed or, if it is employed, the use is common, routine, generally understood, or obvious to a reasonable individual;

(D) any adverse processing impact experienced by an individual as a result of the processing can be resolved easily, with minimal or no effort, and no financial impact; and

(E) processing is for one-time transactions or periodic, known transactions.

(3) MODERATE.—The risk categorization level for a personal data processing activity shall be presumed to be no less than moderate if the processing activity involves any one of the following—

(A) social security numbers, passport numbers, driver's license numbers, or any other unique government-issued identification number linked to a form of identification commonly used to identify, authenticate, or verify the identity of an individual for the purpose of financial transactions, travel, employment, security, proof of age or citizenship, or other similar events;

(B) unique account numbers together with any required security code, access code, or security question or password necessary to access an individual's account;

(C) characteristics of protected classifications under federal law;

(D) tracking precise geospatial information generated from an individual's device;

(E) biometric information tracking or otherwise processing biometric information to identify an individual;

(F) personal data about an individual's physical health;

(G) a decision that impacts an individual based on automated processing without human intervention; or

(H) the first-time commercial application of a technology, business operation, or method of processing.

(4) HIGH.—The risk categorization level for a personal data processing activity shall be presumed to be no less than high if the processing activity involves any one of the following—

(A) reasonable risk of physical harm;

(B) personal data from children under 13;

(C) reasonable risk of financial or economic harm;

(D) eligibility determinations for a right, privilege, or benefit related to employment (including hiring, firing, promotion, demotion, reassignment, or compensation), credit and insurance (including denial of an application, obtaining less favorable terms, cancellation, or an unfavorable change in terms of coverage), housing, education, professional certification, issuance of a license, or the provision of health care and related services;

(E) systemic and continuous observation or monitoring of an individual;

(F) processing related to activities inside an individual's home or equivalent location where an individual has a reasonable expectation of privacy, including a hotel room, rented room, locker room, dressing room, restroom, mobile home, or interior cabin of an individual's personal automobile;

(G) ongoing, persistent, and systemic processing of an individual's precise location information over time and the mapping of the individual's precise location to specific addresses, establishments, or physical locations visited by the individual;

(H) the content of communications;

(I) personal data related to an individual's mental or behavioral health;

(J) personal data related to an individual's sexual life, including sexual activity, sexual orientation, sexual preference, and/or sexual behavior; or

(K) issuing, copying, reproducing, or other processing of identity documents (as opposed to the number associated with the document) such as a driver's license, passport, birth certificate, military ID, other government-issued identity card, or identification related to government or other employment.

(5) EXTREME.—A personal data processing activity shall be presumed to have a risk categorization level of extreme if the processing involves risk of adverse processing impact such as—

(A) loss of life;

(B) life threatening or incapacitating injury, illness, or health condition;

(C) restriction of freedom, including incarceration, quarantine, involuntary commitment, limitations on travel or movement, or forced relocation;

(D) separation or isolation from family members; or

(E) infringement of a right guaranteed by the Constitution of the United States.

(c) When classifying risk, a covered entity shall select the higher risk categorization if there is doubt as to the appropriate classification between two risk levels.

(d) No covered entity shall be held liable for a violation of this Act solely for incorrectly categorizing the level of risk for a particular processing activity if the covered entity establishes by a preponderance of the evidence that the covered entity maintained reasonable procedures to identify, assess, document, and mitigate risk as required by Article V of this Act.

Section 5.04 PROCESSING IMPACT ASSESSMENTS.

(a) A covered entity shall develop, implement, and document policies and procedures for conducting a processing impact assessment to—

(1) ensure that processing conforms to applicable requirements;

(2) determine the risks associated with a processing activity, including processing risk; and

(3) evaluate ways to mitigate such risks.

(b) A covered entity shall conduct and document each processing impact assessment with sufficient clarity and specificity to demonstrate that the covered entity fully considered processing risk and incorporated appropriate controls to mitigate risk throughout the lifecycle of the personal data and processing activity.

(c) A covered entity shall conduct and document a processing impact assessment when, at a minimum, the processing of personal data—

(1) is reasonably likely to create a moderate or greater level of processing risk;

(2) involves new or novel methods of automated processing for observed or inferred data, or a material change to such processing;

(3) is conducted for a legitimate use as defined in Sections 2.01(b)(7) and 2.01(b)(8) of this Act; or

(4) does not produce a benefit to the individual as set forth in Section 2.02(d) of this Act.

(d) At a minimum, a processing impact assessment shall analyze and explain—

(1) the purpose, mission, business needs, and objectives of the processing activity;

(2) the functional needs or capabilities of the processing activity;

(3) the personal data processed;
(4) the entity or entities, including third parties and services providers, involved with the processing;
(5) the category of individuals, groups, or communities that may be impacted;
(6) the assessment of processing risk before measures are taken to mitigate risk;
(7) the controls, safeguards, and other measures implemented to mitigate risk;
(8) the final assessment of residual processing risk remaining after all practicable and reasonable measures are taken to mitigate risk; and
(9) the covered entity's decision to accept the residual processing risk and authorize the processing, as required by Section 5.04(f) of this Act.

(e) Processing impact assessments shall be reviewed and updated on an ongoing basis to ensure they are accurate and current pursuant to a review schedule determined and documented by the covered entity as part of the covered entity's risk management program.

(f) DECISION TO APPROVE AND AUTHORIZE PROCESSING.—

(1) In order to promote accountability and consistency, a covered entity shall develop and document procedures to approve and authorize processing or material modifications in processing as part of the processing impact assessment.
(2) Such procedures shall include a documented framework to enable a covered entity to make an informed, explicit, and justifiable decision to process after considering—
(A) the level of processing risk, including an analysis of residual processing risk;
(B) identifiable risk from forgoing a processing activity;
(C) benefits to the individual; and
(D) societal benefits.
(3) To the extent a covered entity authorizes and approves the processing that is reasonably likely to create a high or greater level of processing risk, a covered entity shall explain why the factors that support processing are not outweighed or counterbalanced by the residual high or greater level of processing risk.

Section 5.05 ENHANCED PROCESSING IMPACT ASSEMEMENT TO ASSESS IMPLICATIONS OF AUTOMATED PROCESSING.

(a) A covered entity shall conduct an enhanced processing impact assessment when the covered entity engages in automated processing that is reasonably likely to create a moderate or greater level of processing risk.

(b) An enhanced processing impact assessment shall examine the full range of interests of parties potentially impacted by processing, including processing risk and potential benefits, including societal benefits.

(c) At a minimum, an enhanced processing impact assessment shall, in addition to the requirements set forth in Section 5.04 of this Act—

(1) enable a relevant employee or other person to see how and why models make the recommendations they do;

(2) provide attestation that analytic models and insights have been tested, to the extent practicable, for accuracy and predictability;

(3) identify the specific individual or body who has ultimate decision-making authority for the automated processing activity;

(4) detect and proactively mitigate bias, to ensure the performance of models is fair, including potential bias that may develop or evolve as models learn or adapt to new experiences or stimuli;

(5) determine the useful life of each insight generated by automated decisions;

(6) explain how the covered entity considered and implemented the requirements set forth in Section 4.04 of this Act; and

(7) confirm that an appropriate mechanism has been established to enable an individual to challenge an adverse outcome created by automated processing as required by Section 3.06(c) of this Act.

Section 5.06 BAD FAITH.—With respect to processing that begins after the effective date of this Act, it shall be unlawful, and an independent and separate violation of this Act to—

(a) misrepresent, expressly or by implication, that a processing impact assessment or enhanced processing impact assessment was completed before the commencement of processing; or

(b) produce a processing impact assessment or enhanced processing impact assessment for the purpose of justifying and documenting a decision that was previously made without evaluating processing risk as required by this Act.

Section 5.07 RULEMAKING.—The Commission shall, within 1 year of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations to provide additional clarification with respect to assessment and categorization of processing risk consistent with the purposes of this Act.

Article VI. INDIVIDUAL PARTICIPATION, MEANINGFUL CONTROL, AND REDRESS

Section 6.01 ACCESS.

(a) ACCESS.—An individual shall be entitled to request and obtain from a covered entity access to the individual's personal data as provided for in Section 3.04 of this Act.

(b) DATA PORTABILITY.—An individual shall be entitled to transmit or transfer personal data to another entity as required by Section 3.05.

Section 6.02 INDIVIDUAL CONTROL.

(a) OPPORTUNITY TO OPT OUT.—An individual shall be provided with the ability to opt out of the use of the individual's personal data as required in Section 3.02(a) of this Act.

(b) INFORMED CONSENT FOR EXTREME RISK.—An individual shall be provided with an opportunity to grant informed consent, and shall grant such consent, before a covered entity may process that individual's personal data where the processing is likely to create an extreme level of processing risk.

(c) ABILITY TO REVOKE CONSENT.—An individual shall be provided with reasonably accessible, conspicuous, and easy-to-use means to withdraw consent as provided for in Section 3.02(d).

(d) DISCONTINUE SHARING WITH THIRD PARTIES.—An individual shall have the opportunity to request that the covered entity discontinue the sharing or disclosure of the individual's personal data as provided for in Section 3.02(e).

Section 6.03 OPPORTUNITY TO SEEK AND OBTAIN MEANINGFUL REDRESS.

(a) OPPORTUNITY TO CORRECT OR AMEND.—An individual shall be entitled to correct or supplement erroneous, incomplete, or inaccurate personal data as provided for in Section 3.06(a).

(b) DELETE PERSONAL DATA.—An individual shall have the opportunity to obtain deletion, to the extent practicable, of personal data relating to the individual as provided for in Section 3.06(b).

(c) CHALLENGE AUTOMATED PROCESSING.—An individual may challenge an adverse outcome of automated processing as provided for in Section 3.06(c).

(d) SUBMIT COMPLAINT OR INQUIRY.—An individual shall be provided with a mechanism to submit a complaint or inquiry regarding a covered entity's policies and procedures relating to the processing of the individual's personal data or compliance with this Act, as required by Section 3.06(d).

Article VII. ENFORCEMENT, OVERSIGHT, AND RULEMAKING

Section 7.01 ENFORCEMENT BY COMMISSION.

(a) IN GENERAL.—A violation of this Act or any regulation prescribed under this Act shall be treated as a violation of a rule under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a) regarding unfair or deceptive acts or practices. Except where the Commission has been expressly granted additional authority under this Act, the Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(b) CIVIL PENALTIES.—

(1) Any covered entity, other than a non-profit organization as defined in Section 1.03(d)(1)(C) of this Act, who violates the specific provisions of this Act as set forth in Section 7.01(b)(3) below or any regulation prescribed under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act as though all applicable terms

and provisions of the Federal Trade Commission Act were incorporated into and made a part of this Act.

(2) In considering whether a civil penalty is in the public interest, the Commission shall consider—

(A) the gravity of the violation, including whether the act or omission for which such penalty is assessed involved fraud, deceit, manipulation, bad faith, or deliberate or reckless disregard of a regulatory requirement;

(B) the severity of adverse processing impact to individuals resulting either directly or indirectly from such act or omission;

(C) the history of previous violations;

(D) the size, financial resources, and good faith of the covered entity charged;

(E) the need to deter such covered entity from committing such acts or omissions; and

(F) such other matters as justice may require.

(3) VIOLATIONS SUBJECT TO CIVIL PENALTIES.—

(A) Upon the effective date of this Act, a covered entity may be subject to civil penalties for violations of Sections 2.01(a), 2.01(d), 2.02(a), 2.02(b), 2.02(c), 2.03, 3.01(a), 3.01(b), 3.02, 3.04(a)(1), 3.04(a)(2), 3.04(b), 3.06(a), 3.07, 4.01(b), 4.02(b), 4.04, 4.05, 4.06(d), 6.01(a), 6.02, and 6.03(d).

(B) Upon the effective date of this Act, a covered entity engaged in processing that creates a high or greater level of processing risk may be subject to civil penalties for violations of Section 4.01(c), 4.01(d), 4.02(c), and 5.06.

(C) In addition to the civil penalties provided for in 7.02(b)(1) and 7.02(b)(3) above, beginning 2 years after the effective date of this Act, a covered entity may be subject to civil penalties for violations of Sections 2.02(d), 3.01(c), 3.01(d), 3.04(a)(3), 3.04(a)(4), 3.04(c), 3.05, 3.06(b), 3.06(c), 3.06(e), 4.03, 4.06(c), 5.04, 5.05, 5.06, 6.01(b), 6.01(b), and 6.03(c).

(4) CIVIL PENALTY CAP.—

(A) Notwithstanding Sections 7.01(b)(1) and (3) above, no civil penalty shall be imposed under this Act in excess of $1,000,000,000 arising out of the same acts or omissions.

(B) The civil penalty cap set forth in this Section does not apply to civil penalties related to a violation of a Commission order or otherwise imposed pursuant to statutes or regulations enforced by the Commission.

(c) EQUITABLE RELIEF.—In any action or proceeding brought or instituted by the Commission under this Act, the Commission may seek, and any Federal court using its full equitable powers may grant, such equitable relief that may be appropriate or necessary to obtain monetary or other relief for past harm or injury, to prevent further violations of this Act, or as otherwise may be in the public interest. Such equitable remedies may include—

(1) temporary restraining order;

(2) preliminary or permanent injunction;

(3) cease-and-desist order;

(4) rescission or reformation of contracts;

(5) refund of money or return of property;

(6) redress, restitution, or disgorgement of profits;

(7) public notification requiring that a covered entity make accurate information available through disclosures, direct notification or education, or publish educational information reasonably related to the violations;

(8) other remedies reasonably related to the unlawful practices conducted by the covered entity, as may be necessary to provide complete relief in light of the purposes of this Act or prevent future violations of this Act; and

(9) such other and further equitable relief as the court deems appropriate.

(d) LIABILITY AND ACCOUNTABILITY FOR INDIVIDUALS IN POSTIONS OF AUTHORITY.—

(1) An individual may be liable for a covered entity's violation of this Act upon a showing that the individual had—

(A) authority to direct or control the covered entity's acts or practices; and

(B) actual knowledge of the covered entity's improper acts or practices; or

(C) reckless, sustained, and systematic failure to exercise oversight.

(2) An individual shall not be liable for civil penalties under this Act unless—

(A) the individual knowingly violated this Act; and

(B) the individual's unlawful conduct created a high or greater level of processing risk and caused significant adverse processing impact.

(e) ENFORCEMENT AUTHORITY PRESERVED.—Nothing in this Section shall be construed to affect any authority of the Commission under any other provision of this Act or other law. Remedies provided in this Section are in addition to, and not in lieu of, any other remedy or right of action otherwise provided by this Act or any other provision of law.

(f) STAY OF ENFORCEMENT.—The Commission may stay enforcement of one or more specific provisions of this Act for no more than 1 year after the effective date upon finding that such stay is in the public interest. The stay shall apply to all entities that are authorized to enforce this Act.

(g) JURISDICTION OVER COMMON CARRIERS AND NON-PROFIT ORGANIZATIONS.—Notwithstanding sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall enforce this Act with respect to—

(1) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and

(2) organizations not organized to carry on business for their own profit or that of their members, as defined in Section 1.03(d)(1)(C) of this Act,

(h) INDEPENDENT LITIGATING AUTHORITY.—The Commission is authorized to litigate cases, by its own attorneys, before any federal court or tribunal within the judicial branch of the United States in order to enforce the provisions of this Act and rules thereunder, and includes authority to commence, defend, intervene in, or appeal any action, suit, or proceeding to which the Commission is a party; enter and enforce orders issued for violations of this Act; litigate court orders related to proceedings to enforce this Act; and argue appeals of such orders or court decisions related to enforcement of this Act.

Section 7.02 ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by any person who violates this Act, the attorney general of the State, as parens patriae,

may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(1) enjoin further violation of this Act by the defendant;

(2) compel compliance with this Act;

(3) obtain damages, restitution, or other compensation on behalf of the residents of the State;

(4) obtain civil penalties in the amount determined and consistent with the requirements under Section 7.01(b) above; and

(5) obtain such other relief as the court using its full equitable powers deems appropriate.

(b) The attorney general of a State shall notify the Commission in writing of any civil action prior to initiating such civil action. Upon receiving notice with respect to a civil action, the Commission may—

(1) intervene in such action; and

(2) upon intervening—

(A) be heard on all matters arising in such civil action; and

(B) file petitions for appeal of a decision in such action.

(3) PREEMPTIVE ACTION BY COMMISSION.—If the Commission institutes a civil action for violation of this Act or a regulation promulgated under this Act, no attorney general of a State may bring a civil action against any defendant named in the complaint of the Commission for violation of this Act or a regulation promulgated pursuant to this Act.

Section 7.03 SAFE HARBOR PROGRAMS FOR RESPONSIBLE AND ACCOUNTABLE COVERED ENTITIES.

(a) COMPLIANCE WITH APPROVED CODES OF CONDUCT.—

(1) Industry organizations, associations, and standards setting bodies may, pursuant to rules promulgated by the Commission, develop enforceable codes of conduct to aid in the application of and compliance with this Act for specific industries or sectors of the economy. A code of conduct may address compliance with the entire Act or may be narrowly tailored to address compliance with one or more Sections of the Act.

(2) A covered entity may comply with such approved code of conduct to satisfy the covered entity's obligations under this Act that correspond with the scope and coverage of the specific code of conduct.

(3) A covered entity that is in compliance with an approved code of conduct and has fully documented such compliance shall not be subject to—

(A) civil penalties for violations of the specific provisions of this Act addressed by the approved code of conduct; or

(B) assessment reviews by the Commission pursuant to Section 7.04.

(4) RULEMAKING.—The Commission shall, within 1 year of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations to implement this Section of the Act. The regulations by the Commission shall, at a minimum, identify the procedures for such codes of conduct to be submitted to the Commission for approval and the criteria by which the Commission shall review, reject, or approve the proposed code in whole or in part.

(b) SAFE HARBOR FOR ACCOUNTABLE SMALL BUSINESS AND NON-PROFIT ORGANIZATIONS.—

(1) A covered entity shall not be subject to enforcement as set forth in Article VII of this Act where the covered entity—

(A) is engaged in interstate commerce and independently owned and operated; or

(B) operates across states and meets the definition of non-profit set forth in section 501 of title 26, United States Code; and

(C) processes personal data of fewer than 50,000 individuals in any 12-month period;

(D) does not derive 50% or more of its annual revenue from selling or licensing personal data; and

(E) engages only in processing that is likely to create no more than a moderate level of processing risk.

(2) MINIMUM REQUIREMENTS.—In order to be subject to the safe harbor, a covered entity shall make a legally enforceable public representation that the covered entity meets the criteria of Section 7.03(b)(1) and has taken reasonable steps to

confirm that the representation is and remains true as long as the covered entity relies on the safe harbor.

Section 7.04 ACCOUNTABILITY REPORTS AND ASSESSMENTS.

(a) AUTHORITY TO OBTAIN INFORMATION AND DOCUMENTS.—

(1) In addition to its existing authority pursuant to the Federal Trade Commission Act and other laws enforced by the Commission, including this Act, the Commission shall have the authority to require, by special orders, a covered entity, other than a non-profit organization as defined in Section 1.03(d)(1)(C) of this Act, to file with the Commission, in such form as the Commission may prescribe, reports or answers in writing to specific questions, furnishing to the Commission such information as it may require as to the covered entity's—

(A) business operations;

(B) processing activities; and

(C) programs, policies, and procedures adopted and implemented by the covered entity to meet the requirements of this Act.

(2) The Commission may seek such information, as it deems necessary to ensure that commercial practices are consistent with the requirements of this Act, assess compliance, determine whether a violation of law exists, gather information necessary to support the report to Congress as required by Section 8.04 of this Act, or for other reports to Congress or the Executive Branch. Information sought must be reasonably relevant to the Commission's mission, the purposes of this Act, and in the public interest. Special orders issued pursuant to this Section shall be reasonable and shall not impose an undue burden on a covered entity.

(3) Reports and answers shall be made under oath, or otherwise, as the Commission may prescribe, and shall be filed with the Commission within such reasonable period as the Commission may prescribe.

(4) The Commission's authority to obtain information pursuant to this Section shall not be subject to the Paperwork Reduction Act (44 U.S.C. 3501-3520).

(b) REVIEW OF RECORDS.—All final records, documents, or assessments required to be made and kept by a covered entity pursuant to this Act are subject at any time,

or from time to time, to such reasonable periodic, special, or other review by representatives of the Commission as the Commission deems necessary or appropriate in the public interest, for the protection of individuals, or otherwise in furtherance of the purposes of this Act.

(c) PROCEDURES.—A covered entity shall have the same right to challenge an order issued pursuant to this Section and seek judicial review of a decision by the Commission as provided for Commission orders issued pursuant to Section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)).

Section 7.05 IMPLEMENTING REGULATIONS TO SUPPORT ACCOUNTABILITY.

(a) AUTHORITY.—The Commission shall, in accordance with section 553 of title 5, United States Code, promulgate regulations to carry out the purposes of this Act.

(b) AUTHORITY TO GRANT EXCLUSIONS.—In promulgating rules under this Act, the Commission may implement such additional exclusions from this Act as the Commission considers consistent with the purposes of this Act and in the public interest.

(c) CRITERIA FOR ISSUANCE OF RULES.—

(1) In promulgating regulations, the Commission shall consider—

(A) the potential benefits and costs to individuals and covered entities, including the potential reduction of access by individuals to products or services resulting from such regulations; and

(B) that compliance with such regulations must allow for flexibility in implementation and be reasonable and appropriate for a covered entity taking into account—

(i) the size, resources, and complexity of the covered entity;

(ii) the nature and scope of the covered entity's processing activities;

(iii) the potential level of processing risk created by such processing; and

(iv) the burden on a covered entity that is a non-profit organization as defined in Section 1.03(d)(1)(A) of this Act.

(d) In promulgating such regulations, the Commission shall not require the deployment or use of any specific products or technologies, including any specific

computer software or hardware, nor prescribe or otherwise require that computer software or hardware products or services be designed, developed, or manufactured in a particular manner.

Article VIII. COMMISSION EDUCATION, GUIDANCE, OUTREACH, AND REPORTS

Section 8.01 CONSUMER EDUCATION.—

(a) RESOURCES FOR CONSUMERS.—In order to protect individuals' personal information and to ensure that individuals have the confidence to take advantage of the many benefits of products offered in the marketplace, the Commission shall publish resources to educate individuals with respect to—

(1) the various ways an individual may interact with processing as well as devices and technology that enable processing including the collection of personal data;

(2) the potential benefits and risks, including risk of adverse processing impact, that may be associated with processing in order to help individuals make more informed decisions;

(3) helping individuals compare the processing activities of different digital products and services; and

(4) helping individuals understand their options with respect to processing by a covered entity provided for by this Act.

(b) EDUCATION INITIATIVES FOR OLDER AMERICANS.—The Commission shall—

(1) engage in activities designed to facilitate the digital literacy of individuals who have attained the age of 62 years or more, including through the dissemination of materials to help such individuals protect and control their personal data, safely and effectively use new technology and devices necessary to engage in society, and understand their options with respect to processing by a covered entity;

(2) work with community organizations, non-profit organizations, and other entities that are involved with educating or assisting individuals who have attained the age of 62 years or more; and

(3) coordinate efforts to protect individuals who have attained the age of 62 years or more with other Federal agencies and State regulators, as appropriate, to promote consistent, effective, and efficient enforcement.

Section 8.02 GUIDANCE AND OUTREACH FOR COVERED ENTITIES.

(a) GUIDANCE.—The Commission shall publish guidance, training materials, proposed best practices, and other resources designed to assist covered entities with coming into compliance with obligations under this Act, taking into account that the requirements of this Act are intended to be flexible and scalable to accommodate the range in types and sizes of covered entities that must comply with the provisions of this Act.

(b) SMALL BUSINESS SUPPORT.—Recognizing that small businesses make up a large and vital segment of the U.S. economy, the Commission shall develop and implement guidance and resources specifically designed to help small businesses meet their obligations under this Act and shall undertake outreach efforts to ensure that small businesses are aware of their obligations under the Act and the resources available to support small businesses.

(c) The Commission shall establish a mechanism for a covered entity to submit an inquiry to the Commission regarding compliance with this Act. To the extent practicable and in the public interest, the Commission shall make available to the public the Commission's responses to such inquiries and shall take such inquiries into account when developing guidance and educational materials for covered entities. Responses may take the form of a Commission staff opinion letter, or such other form as the Commission determines meets the objectives of this Section and purposes of this Act.

Section 8.03 INTERNATIONAL COOPERATION FOR THE PROTECTION OF PERSONAL DATA.—The Commission shall, consistent with its current authorities, endeavor to cooperate and coordinate with foreign agencies and provide such agencies with information regarding this Act to foster—

(a) understanding of the protections for personal data and individuals under this Act;

(b) consistency in the interpretation and enforcement for the protection of personal data; and

(c) cooperation and convergence toward best practices with respect to processing covered by this Act.

Section 8.04 REPORT.—Not later than 3 years after the date of enactment of this Act, the Commission shall transmit to Congress a report describing the Commission's use of and experience with the authority granted by this Act, along with any recommendations for revisions to the Act or additional legislation. The report shall include—

(a) the number of complaints related to the processing of personal data or alleged violations of this Act received by the Commission;

(b) the number of investigations initiated by the Commission related to the processing of personal data and suspected violations of this Act;

(c) the number of enforcement actions initiated by the Commission for alleged violations of this Act and a summary of such enforcement actions;

(d) the Commission's efforts to coordinate with State Attorneys General regarding enforcement of this Act;

(e) the status of any rulemaking proceedings undertaken pursuant to this Act;

(f) the Commission's efforts to provide guidance to covered entities, including small sized covered entities as provided for in Section 8.02(b) of this Act;

(g) the Commission's efforts to provide education to individuals as provided for in Sections 8.01 of this Act;

(h) the Commission's efforts to support the effective implementation and application of the safe harbor provisions of this Act, including approval of codes of conduct, as provided for in Section 7.03 of this Act;

(i) the Commission's exercise of its authority under Section 7.04 of this Act to undertake assessment reviews; and

(j) Commission resources allocated to the implementation and enforcement of this Act and an assessment of the adequacy of such resources.

Article IX. COMMISSION RESOURCES AND AUTHORIZATION OF APPROPRIATIONS

Section 9.01 APPOINTMENT OF ADDITIONAL PERSONNEL.—Notwithstanding any other provision of law, the Chair of the Commission may, without regard to the civil service laws (including regulations), appoint additional personnel for the purpose of enforcing this Act and otherwise meeting the Commission's obligations under this Act, including—

(a) 250 additional personnel in attorney positions; and

(b) 250 additional personnel in project management, technical, and administrative support positions.

Section 9.02 AUTHORITY TO ESTABLISH NEW BUREAU OR OFFICE.—The attorneys and support personnel appointed pursuant to Article IV of this Act shall be assigned to the Bureau of Consumer Protection or such other bureau or office as the Chair may create, taking into account—

(a) the efficient and effective application of Commission resources;

(b) avoidance of duplicative functions;

(c) impact on the Commission's ability to carry out its dual mission of protecting consumers and promoting competition; and

(d) the public interest.

Section 9.03 AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commission such sums as may be necessary to carry out this Act.

Article X. PREEMPTION

Section 10.01 PREEMPTION.—For a covered entity subject to this Act, the provisions of this Act shall preempt any civil provisions of the law of any State or political subdivision of a State to the degree they are focused on the reduction of processing risk through the regulation of personal data processing activities.

Section 10.02 EFFECT ON OTHER LAWS.

(a) CONSUMER PROTECTION LAWS.—Except as provided in Section 10.01, this Act shall not be construed to limit the enforcement, or the bringing of a claim

pursuant to any State consumer protection law by an attorney general of a State, other than to the extent to which those laws regulate personal data collection and processing.

(b) PROTECTION OF CERTAIN STATE LAW.—Nothing in this Act shall be construed to preempt the applicability of—

(1) the constitutional, trespass, contract, data breach notification, or tort law of any state, other than to the degree such laws are substantially intended to govern personal data collection and processing;

(2) any other state law to the extent that the law relates to acts of fraud, wiretapping, or the protection of social security numbers;

(3) any state law to the extent it provides additional provisions to specifically regulate the covered entities as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–91), the Family Educational Rights and Privacy Act (Public Law 93–380), the Fair Credit Reporting Act (Public Law 91–508) or the Financial Services Modernization Act of 1999 (Public Law 106–102); or

(4) private contracts based on any state law that require a party to provide additional or greater protections to an individual than does this Act.

(c) PRESERVATION OF COMMISSION AUTHORITY.—Nothing in this Act shall be construed to in any way limit the authority of the Commission under any other provision of law.

(d) FCC AUTHORITY.—Insofar as any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.), including section 222 of the Communications Act of 1934 (47 U.S.C. 222), or any regulations promulgated under such Act, apply to any person subject to this Act with respect to privacy policies, terms of service, and practices covered by this Act, such provision of the Communications Act of 1934 or such regulations shall have no force or effect, unless such regulations pertain to emergency services.

(e) TREATMENT OF COVERED ENTITIES GOVERNED BY OTHER FEDERAL LAW.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–91), the Family Educational Rights and Privacy Act

(Public Law 93–380), the Fair Credit Reporting Act (Public Law 91–508), or the Financial Services Modernization Act of 1999 (Public Law 106–102), are excluded from the provisions of this Act to the degree specific uses of personal data are covered by the relevant provisions of those laws.

Section 10.03 GOVERNMENT ACCOUNTABILITY OFFICE STUDY AND REPORT.—Not later than 3 years after the effective date of this Act, the Comptroller General of the United States shall submit to the President and Congress a report that surveys federal privacy and security laws that—

(a) identifies inconsistencies between this Act and other federal privacy and security laws; and

(b) provides recommendations to modify, amend, or rescind provisions of this Act or provisions of other federal laws in order to avoid or eliminate inconsistent, contradictory, duplicative, or outdated legal requirements that may no longer be relevant or necessary to protect consumers in light of this Act, rules thereunder, and changing technological and economic trends.

Article XI. EFFECTIVE DATE AND SAVINGS CLAUSE.

Section 11.01 EFFECTIVE DATE.—The provisions of this Act that apply to covered entities shall apply beginning on or after the date that is 2 years from the date of enactment of this Act.

Section 11.02 NO RETROACTIVE APPLICABILITY.—This Act shall not apply to any conduct that occurred before the effective date under Section 11.01 above.

Section 11.03 SAVINGS CLAUSE.—If any provision of this Act, an amendment made by this Act, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this Act, the amendments made by this Act, and the application of the provisions of such to any person or circumstance shall not be affected thereby.