HOUSE DOCKET, NO. 4053 FILED ON: 1/17/2025

HOUSE . . . . . No.

The Commonwealth of Massachusetts

PRESENTED BY:

David M. Rogers and Andres X. Vargas

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act protecting consumers in interactions with artificial intelligence systems.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
David M. Rogers	*24th Middlesex*	*1/17/2025*
Andres X. Vargas	*3rd Essex*	*1/17/2025*

HOUSE DOCKET, NO. 4053 FILED ON: 1/17/2025

HOUSE . . . . . No.

[Pin Slip]

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act protecting consumers in interactions with artificial intelligence systems.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws, as appearing in the 2022 Official Edition, are hereby amended by inserting a new chapter:

CHAPTER 93M. Consumer Protections in interactions with Artificial Intelligence Systems

Section 1. Definitions

The following words shall, unless the context clearly requires otherwise, have the following meanings:—

"Algorithmic discrimination" means any condition in which the use of an artificial intelligence system results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race,

religion, reproductive health, sex, veteran status, or other classification protected under the laws of this state or federal law.

"Algorithmic discrimination" does not include:

(1) the offer, license, or use of a high-risk artificial intelligence system by a developer or deployer for the sole purpose of:

(i) the developer's or deployer's self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with state and federal law; or

(ii) expanding an applicant, customer, or participant pool to increase diversity or redress historical discrimination; or

(2) an act or omission by or on behalf of a private club or other establishment that is not in fact open to the public, as set forth in Title II of the federal "Civil Rights Act of 1964", 42 U.S.C. Sec. 2000a (e), as amended.

"Artificial intelligence system" means any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

"Consequential decision" means a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of:

(1) education enrollment or an education opportunity;

(2) employment or an employment opportunity;

(3) a financial or lending service;

(4) an essential government service;

(5) health-care services;

(6) housing;

(7) insurance; or

(8) a legal service.

"Consumer" means an individual who is a Massachusetts resident.

"Deploy" means to use a high-risk artificial intelligence system.

"Deployer" means a person doing business in this state that deploys a high-risk artificial intelligence system.

"Developer" means a person doing business in this state that develops or intentionally and substantially modifies an artificial intelligence system.

"Health-care services" has the same meaning as provided in 42 U.S.C. Sec. 234 (d)(2).

"High-risk artificial intelligence system" means any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision.

"High-risk artificial intelligence system" does not include:

(1) an artificial intelligence system if the artificial intelligence system is intended to:

(i) perform a narrow procedural task; or

(ii) detect decision-making patterns or deviations from prior decision-making patterns and is not intended to replace or influence a previously completed human assessment without sufficient human review; or

(2) the following technologies, unless the technologies, when deployed, make, or are a substantial factor in making, a consequential decision:

(i) anti-fraud technology that does not use facial recognition technology;

(ii) anti-malware;

(iii) anti-virus;

(iv) artificial intelligence-enabled video games;

(v) calculators;

(vi) cybersecurity;

(vii) databases;

(viii) data storage;

(ix) firewall;

(x) internet domain registration;

(xi) internet website loading;

(xii) networking;

(xiii) spam- and robocall-filtering;

(xiv) spell-checking;

(xv) spreadsheets;

(xvi) web caching;

(xvii) web hosting or any similar technology; or

(xviii) technology that communicates with consumers in natural language for the purpose of providing users with information, making referrals or recommendations, and answering questions and is subject to an accepted use policy that prohibits generating content that is discriminatory or harmful.

"Intentional and substantial modification" or "intentionally and substantially modifies" means a deliberate change made to an artificial intelligence system that results in any new reasonably foreseeable risk of algorithmic discrimination.

"Intentional and substantial modification" or "intentionally and substantially modifies" does not include a change made to a high-risk artificial intelligence system, or the performance of a high-risk artificial intelligence system, if:

(1) the high-risk artificial intelligence system continues to learn after the high-risk artificial intelligence system is:

(i) offered, sold, leased, licensed, given, or otherwise made available to a deployer; or

(ii) deployed;

(2) the change is made to the high-risk artificial intelligence system as a result of any learning described in paragraph (1)(i) of this subsection;

(3) the change was predetermined by the deployer, or a third party contracted by the deployer, when the deployer or third party completed an initial impact assessment of such high-risk artificial intelligence system pursuant to section 3 (c) (1); and

(4) the change is included in technical documentation for the high-risk artificial intelligence system.

"Substantial factor" means a factor that:

(1) assists in making a consequential decision;

(2) is capable of altering the outcome of a consequential decision; and

(3) is generated by an artificial intelligence system.

"Substantial factor" includes any use of an artificial intelligence system to generate any content, decision, prediction, or recommendation concerning a consumer that is used as a basis to make a consequential decision concerning the consumer.

"Trade secret" has the meaning set forth in section 42 (4) of chapter 93 of the General Laws, as appearing in the 2022 Official Edition.

Section 2. Developer duty to avoid algorithmic discrimination - required documentation.

(a) Not later than 6 months after the effective date of this act, a developer of a high-risk artificial intelligence system shall use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended and contracted uses of the high-risk artificial intelligence system. In any enforcement action brought not later than 6 months after the effective date of this act, by the attorney general pursuant to

section 6, there is a rebuttable presumption that a developer used reasonable care as required under this section if the developer complied with this section and any additional requirements or obligations as set forth in rules promulgated by the attorney general pursuant to section 7.

(b) Not later than 6 months after the effective date of this act, and except as provided in subsection (f) of this section, a developer of a high-risk artificial intelligence system shall make available to the deployer or other developer of the high-risk artificial intelligence system:

(1) a general statement describing the reasonably foreseeable uses and known harmful or inappropriate uses of the high-risk artificial intelligence system;

(2) documentation disclosing:

(i) high-level summaries of the type of data used to train the high-risk artificial intelligence system;

(ii) known or reasonably foreseeable limitations of the high-risk artificial intelligence system, including known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of the high-risk artificial intelligence system;

(iii) the purpose of the high-risk artificial intelligence system;

(iv) the intended benefits and uses of the high-risk artificial intelligence system; and

(v) all other information necessary to allow the deployer to comply with the requirements of section 3;

(3) documentation describing:

(i) how the high-risk artificial intelligence system was evaluated for performance and mitigation of algorithmic discrimination before the high-risk artificial intelligence system was offered, sold, leased, licensed, given, or otherwise made available to the deployer;

(ii) the data governance measures used to cover the training datasets and the measures used to examine the suitability of data sources, possible biases, and appropriate mitigation;

(iii) the intended outputs of the high-risk artificial intelligence system;

(iv) the measures the developer has taken to mitigate known or reasonably foreseeable risks of algorithmic discrimination that may arise from the reasonably foreseeable deployment of the high-risk artificial intelligence system; and

(v) how the high-risk artificial intelligence system should be used, not be used, and be monitored by an individual when the high-risk artificial intelligence system is used to make, or is a substantial factor in making, a consequential decision; and

(4) any additional documentation that is reasonably necessary to assist the deployer in understanding the outputs and monitor the performance of the high-risk artificial intelligence system for risks of algorithmic discrimination.

(c) (1) except as provided in subsection (f) of this section, a developer that offers, sells, leases, licenses, gives, or otherwise makes available to a deployer or other developer a high-risk artificial intelligence system not later than 6 months after the effective date of this act, shall make available to the deployer or other developer, to the extent feasible, the documentation and information, through artifacts such as model cards, dataset cards, or other impact assessments,

necessary for a deployer, or for a third party contracted by a deployer, to complete an impact assessment pursuant to section 3 (c).

(2) a developer that also serves as a deployer for a high-risk artificial intelligence system is not required to generate the documentation required by this section unless the high-risk artificial intelligence system is provided to an unaffiliated entity acting as a deployer.

(d) (1) Not later than 6 months after the effective date of this act, a developer shall make available, in a manner that is clear and readily available on the developer's website or in a public use case inventory, a statement summarizing:

(i) the types of high-risk artificial intelligence systems that the developer has developed or intentionally and substantially modified and currently makes available to a deployer or other developer; and

(ii) how the developer manages known or reasonably foreseeable risks of algorithmic discrimination that may arise from the development or intentional and substantial modification of the types of high-risk artificial intelligence systems described in accordance with subsection (d)(1)(i) of this section.

(2) a developer shall update the statement described in subsection (d)(1) of this section:

(i) as necessary to ensure that the statement remains accurate; and

(ii) no later than ninety days after the developer intentionally and substantially modifies any high-risk artificial intelligence system described in subsection (d)(1)(i) of this section.

(e) Not later than 6 months after the effective date of this act, a developer of a high-risk artificial intelligence system shall disclose to the attorney general, in a form and manner

prescribed by the attorney general, and to all known deployers or other developers of the high-risk artificial intelligence system, any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of the high-risk artificial intelligence system without unreasonable delay but no later than ninety days after the date on which:

(1) the developer discovers through the developer's ongoing testing and analysis that the developer's high-risk artificial intelligence system has been deployed and has caused or is reasonably likely to have caused algorithmic discrimination; or

(2) the developer receives from a deployer a credible report that the high-risk artificial intelligence system has been deployed and has caused algorithmic discrimination.

(f) nothing in subsections (b) to (e) of this section requires a developer to disclose a trade secret, information protected from disclosure by state or federal law, or information that would create a security risk to the developer.

(g) Not later than 6 months after the effective date of this act, the attorney general may require that a developer disclose to the attorney general, no later than ninety days after the request and in a form and manner prescribed by the attorney general, the statement or documentation described in subsection (b) of this section. The attorney general may evaluate such statement or documentation to ensure compliance with this chapter, and the statement or documentation is not subject to disclosure under the “Massachusetts Public Records Law”, chapter 66, section 10 of the General Laws. In a disclosure pursuant to this subsection (g), a developer may designate the statement or documentation as including proprietary information or a trade secret. To the extent that any information contained in the statement or documentation

includes information subject to attorney-client privilege or work-product protection, the disclosure does not constitute a waiver of the privilege or protection.

Section 3. Deployer duty to avoid algorithmic discrimination - risk management policy and program.

(a) Not later than 6 months after the effective date of this act, a deployer of a high-risk artificial intelligence system shall use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination. In any enforcement action brought not later than 6 months after the effective date of this act, by the attorney general pursuant to section 6, there is a rebuttable presumption that a deployer of a high-risk artificial intelligence system used reasonable care as required under this section if the deployer complied with this section and any additional requirements or obligations as set forth in rules promulgated by the attorney general pursuant to section 7.

(b) (1) Not later than 6 months after the effective date of this act, and except as provided in subsection (f) of this section, a deployer of a high-risk artificial intelligence system shall implement a risk management policy and program to govern the deployer's deployment of the high-risk artificial intelligence system. The risk management policy and program must specify and incorporate the principles, processes, and personnel that the deployer uses to identify, document, and mitigate known or reasonably foreseeable risks of algorithmic discrimination. The risk management policy and program must be an iterative process planned, implemented, and regularly and systematically reviewed and updated over the life cycle of a high-risk artificial intelligence system, requiring regular, systematic review and updates. A risk management policy

and program implemented and maintained pursuant to this subsection (b) must be reasonable considering:

(i) (A) the guidance and standards set forth in the latest version of the "Artificial Intelligence Risk Management Framework" published by the National Institute of Standards and Technology in the United States Department of Commerce, standard ISO/IEC 42001 of the International Organization for Standardization, or another nationally or internationally recognized risk management framework for artificial intelligence systems, if the standards are substantially equivalent to or more stringent than the requirements of this chapter; or

(B) any risk management framework for artificial intelligence systems that the attorney general, in the attorney general's discretion, may designate;

(ii) the size and complexity of the deployer;

(iii) the nature and scope of the high-risk artificial intelligence systems deployed by the deployer, including the intended uses of the high-risk artificial intelligence systems; and

(iv) the sensitivity and volume of data processed in connection with the high-risk artificial intelligence systems deployed by the deployer.

(2) a risk management policy and program implemented pursuant to subsection (b)(1) of this section may cover multiple high-risk artificial intelligence systems deployed by the deployer.

(c) (1) except as provided in subsections (c)(4), (c)(5), and (f) of this section:

(i) a deployer, or a third party contracted by the deployer, that deploys a high-risk artificial intelligence system not later than 6 months after the effective date of this act, shall complete an impact assessment for the high-risk artificial intelligence system; and

(ii) Not later than 6 months after the effective date of this act, a deployer, or a third party contracted by the deployer, shall complete an impact assessment for a deployed high-risk artificial intelligence system at least annually and within ninety days after any intentional and substantial modification to the high-risk artificial intelligence system is made available.

(2) an impact assessment completed pursuant to this subsection (c) must include, at a minimum, and to the extent reasonably known by or available to the deployer:

(i) a statement by the deployer disclosing the purpose, intended use cases, and deployment context of, and benefits afforded by, the high-risk artificial intelligence system;

(ii) an analysis of whether the deployment of the high-risk artificial intelligence system poses any known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature of the algorithmic discrimination and the steps that have been taken to mitigate the risks;

(iii) a description of the categories of data the high-risk artificial intelligence system processes as inputs and the outputs the high-risk artificial intelligence system produces;

(iv) if the deployer used data to customize the high-risk artificial intelligence system, an overview of the categories of data the deployer used to customize the high-risk artificial intelligence system;

(v) any metrics used to evaluate the performance and known limitations of the high-risk artificial intelligence system;

(vi) a description of any transparency measures taken concerning the high-risk artificial intelligence system, including any measures taken to disclose to a consumer that the high-risk artificial intelligence system is in use when the high-risk artificial intelligence system is in use; and

(vii) a description of the post-deployment monitoring and user safeguards provided concerning the high-risk artificial intelligence system, including the oversight, use, and learning process established by the deployer to address issues arising from the deployment of the high-risk artificial intelligence system.

(3) in addition to the information required under subsection (3)(b) of this section, an impact assessment completed pursuant to this subsection (c) following an intentional and substantial modification to a high-risk artificial intelligence system not later than 6 months after the effective date of this act, must include a statement disclosing the extent to which the high-risk artificial intelligence system was used in a manner that was consistent with, or varied from, the developer's intended uses of the high-risk artificial intelligence system.

(4) a single impact assessment may address a comparable set of high-risk artificial intelligence systems deployed by a deployer.

(5) if a deployer, or a third party contracted by the deployer, completes an impact assessment for the purpose of complying with another applicable law or regulation, the impact assessment satisfies the requirements established in this subsection (c) if the impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this subsection (c).

(6) a deployer shall maintain the most recently completed impact assessment for a high-risk artificial intelligence system as required under this subsection (c), all records concerning each impact assessment, and all prior impact assessments, if any, for at least three years following the final deployment of the high-risk artificial intelligence system.

(7) Not later than 6 months after the effective date of this act, and at least annually thereafter, a deployer, or a third party contracted by the deployer, must review the deployment of each high-risk artificial intelligence system deployed by the deployer to ensure that the high-risk artificial intelligence system is not causing algorithmic discrimination.

(d) (1) Not later than 6 months after the effective date of this act, and no later than the time that a deployer deploys a high-risk artificial intelligence system to make, or be a substantial factor in making, a consequential decision concerning a consumer, the deployer shall:

(i) notify the consumer that the deployer has deployed a high-risk artificial intelligence system to make, or be a substantial factor in making, a consequential decision before the decision is made;

(ii) provide to the consumer a statement disclosing the purpose of the high-risk artificial intelligence system and the nature of the consequential decision; the contact information for the deployer; a description, in plain language, of the high-risk artificial intelligence system; and instructions on how to access the statement required by subsection (5)(a) of this section; and

(iii) provide to the consumer information, if applicable, regarding the consumer's right to opt out of the processing of personal data concerning the consumer for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(2) Not later than 6 months after the effective date of this act, a deployer that has deployed a high-risk artificial intelligence system to make, or be a substantial factor in making, a consequential decision concerning a consumer shall, if the consequential decision is adverse to the consumer, provide to the consumer:

(i) a statement disclosing the principal reason or reasons for the consequential decision, including:

(A) the degree to which, and manner in which, the high-risk artificial intelligence system contributed to the consequential decision;

(B) the type of data that was processed by the high-risk artificial intelligence system in making the consequential decision; and

(C) the source or sources of the data described in subsection (d)(2)(i)(B) of this section;

(ii) an opportunity to correct any incorrect personal data that the high-risk artificial intelligence system processed in making, or as a substantial factor in making, the consequential decision; and

(iii) an opportunity to appeal an adverse consequential decision concerning the consumer arising from the deployment of a high-risk artificial intelligence system, which appeal must, if technically feasible, allow for human review unless providing the opportunity for appeal is not in the best interest of the consumer, including in instances in which any delay might pose a risk to the life or safety of such consumer.

(3) (i) except as provided in subsection (d)(3)(ii) of this section, a deployer shall provide the notice, statement, contact information, and description required by subsections (c)(1) and (d)(2) of this section:

(A) directly to the consumer;

(B) in plain language;

(C) in all languages in which the deployer, in the ordinary course of the deployer's business, provides contracts, disclaimers, sale announcements, and other information to consumers; and

(D) in a format that is accessible to consumers with disabilities.

(ii) if the deployer is unable to provide the notice, statement, contact information, and description required by subsections (d)(1) and (d)(2) of this section directly to the consumer, the deployer shall make the notice, statement, contact information, and description available in a manner that is reasonably calculated to ensure that the consumer receives the notice, statement, contact information, and description.

(e) (1) Not later than 6 months after the effective date of this act, and except as provided in subsection (f) of this section, a deployer shall make available, in a manner that is clear and readily available on the deployer's website, a statement summarizing:

(i) the types of high-risk artificial intelligence systems that are currently deployed by the deployer;

(ii) how the deployer manages known or reasonably foreseeable risks of algorithmic discrimination that may arise from the deployment of each high-risk artificial intelligence system described pursuant to subsection (e)(1)(i) of this section; and

(iii) in detail, the nature, source, and extent of the information collected and used by the deployer.

(2) a deployer shall periodically update the statement described in subsection (e)(1) of this section.

(f) subsections (b), (c), and (e) of this section do not apply to a deployer if, at the time the deployer deploys a high-risk artificial intelligence system and at all times while the high-risk artificial intelligence system is deployed:

(1) the deployer:

(i) employs fewer than fifty full-time equivalent employees; and

(ii) does not use the deployer's own data to train the high-risk artificial intelligence system;

(2) the high-risk artificial intelligence system:

(i) is used for the intended uses that are disclosed to the deployer as required by section 2 (b)(1); and

(ii) continues learning based on data derived from sources other than the deployer's own data; and

(3) the deployer makes available to consumers any impact assessment that:

(i) the developer of the high-risk artificial intelligence system has completed and provided to the deployer; and

(ii) includes information that is substantially similar to the information in the impact assessment required under of this section.

(g) if a deployer deploys a high-risk artificial intelligence system not later than 6 months after the effective date of this act, and subsequently discovers that the high-risk artificial intelligence system has caused algorithmic discrimination, the deployer, without unreasonable delay, but no later than ninety days after the date of the discovery, shall send subsection (c)(2) to the attorney general, in a form and manner prescribed by the attorney general, a notice disclosing the discovery.

(h) nothing in subsections (b) to (e) and (g) of this section requires a deployer to disclose a trade secret or information protected from disclosure by state or federal law. To the extent that a deployer withholds information pursuant to this subsection (h) or section 5 (e), the deployer shall notify the consumer and provide a basis for the withholding.

(i) Not later than 6 months after the effective date of this act, the attorney general may require that a deployer, or a third party contracted by the deployer, disclose to the attorney general, no later than ninety days after the request and in a form and manner prescribed by the attorney general, the risk management policy implemented pursuant to subsection (b) of this section, the impact assessment completed pursuant to subsection (c) of this section, or the records maintained pursuant to subsection (c)(6) of this section. The attorney general may evaluate the risk management policy, impact assessment, or records to ensure compliance with this chapter, and the risk management policy, impact assessment, and records are not subject to

disclosure under the “Massachusetts Public Records Law”, chapter 66, section 10 of the General Laws. In a disclosure pursuant to this subsection (i), a deployer may designate the statement or documentation as including proprietary information or a trade secret. To the extent that any information contained in the risk management policy, impact assessment, or records include information subject to attorney-client privilege or work-product protection, the disclosure does not constitute a waiver of the privilege or protection.

Section 4. Disclosure of an artificial intelligence system to consumer

(a) Not later than 6 months after the effective date of this act, and except as provided in subsection (b) of this section, a deployer or other developer that deploys, offers, sells, leases, licenses, gives, or otherwise makes available an artificial intelligence system that is intended to interact with consumers shall ensure the disclosure to each consumer who interacts with the artificial intelligence system that the consumer is interacting with an artificial intelligence system.

(b) disclosure is not required under subsection (a) of this section under circumstances in which it would be obvious to a reasonable person that the person is interacting with an artificial intelligence system.

Section 5. Compliance with other legal obligations - definitions

(a) nothing in this chapter restricts a developer's, a deployer's, or other person's ability to:

(1) comply with federal, state, or municipal laws, ordinances, or regulations;

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, a state, a municipal, or other governmental authority;

(3) cooperate with a law enforcement agency concerning conduct or activity that the developer, deployer, or other person reasonably and in good faith believes may violate federal, state, or municipal laws, ordinances, or regulations;

(4) investigate, establish, exercise, prepare for, or defend legal claims;

(5) take immediate steps to protect an interest that is essential for the life or physical safety of a consumer or another individual;

(6) by any means other than the use of facial recognition technology, prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or illegal activity; investigate, report, or prosecute the persons responsible for any such action; or preserve the integrity or security of systems;

(7) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is conducted in accordance with 45 CFR 46, as amended, or relevant requirements established by the federal Food and Drug Administration;

(8) conduct research, testing, and development activities regarding an artificial intelligence system or model, other than testing conducted under real-world conditions, before the artificial intelligence system or model is placed on the market, deployed, or put into service, as applicable; or

(i) assist another developer, deployer, or other person with any of the obligations imposed under this chapter.

(b) the obligations imposed on developers, deployers, or other persons under this chapter do not restrict a developer's, a deployer's, or other person's ability to:

(1) effectuate a product recall; or

(2) identify and repair technical errors that impair existing or intended functionality.

(c) the obligations imposed on developers, deployers, or other persons under this chapter do not apply where compliance with this chapter by the developer, deployer, or other person would violate an evidentiary privilege under the laws of this state.

(d) nothing in this chapter imposes any obligation on a developer, a deployer, or other person that adversely affects the rights or freedoms of a person, including the rights of a person to freedom of speech or freedom of the press that are guaranteed in:

(1) the First Amendment to the United States constitution; or

(2) Part the First, Article XVI of the state constitution.

(e) nothing in this chapter applies to a developer, a deployer, or other person:

(1) insofar as the developer, deployer, or other person develops, deploys, puts into service, or intentionally and substantially modifies, as applicable, a high-risk artificial intelligence system:

(i) that has been approved, authorized, certified, cleared, developed, or granted by a federal agency, such as the federal food and drug administration or the federal aviation administration, acting within the scope of the federal agency's authority, or by a regulated entity subject to the supervision and regulation of the federal housing finance agency; or

(ii) in compliance with standards established by a federal agency, including standards established by the federal office of the national coordinator for health information technology, or by a regulated entity subject to the supervision and regulation of the federal housing finance agency, if the standards are substantially equivalent or more stringent than the requirements of this chapter;

(2) conducting research to support an application for approval or certification from a federal agency, including the federal Aviation Administration, the federal Communications Commission, or the federal Food and Drug Administration or research to support an application otherwise subject to review by the federal agency;

(3) performing work under, or in connection with, a contract with the United States Department of Commerce, the United States Department of Defense, or the National Aeronautics and Space Administration, unless the developer, deployer, or other person is performing the work on a high-risk artificial intelligence system that is used to make, or is a substantial factor in making, a decision concerning employment or housing; or

(4) that is a covered entity within the meaning of the federal "Health Insurance Portability and Accountability Act of 1996", 42 U.S.C. Secs. 1320d to 1320d-9, and the regulations promulgated under the federal act, as both may be amended from time to time, and is providing health-care recommendations that:

(i) are generated by an artificial intelligence system;

(ii) require a health-care provider to take action to implement the recommendations; and

(iii) are not considered to be high risk.

(f) nothing in this chapter applies to any artificial intelligence system that is acquired by or for the federal government or any federal agency or department, including the United States Department of Commerce, the United States Department of Defense, or the National Aeronautics and Space Administration, unless the artificial intelligence system is a high-risk artificial intelligence system that is used to make, or is a substantial factor in making, a decision concerning employment or housing.

(g) an insurer, as defined in chapter 175, a fraternal benefit society, as defined in chapter 176, or a developer of an artificial intelligence system used by an insurer is in full compliance with this chapter if the insurer, the fraternal benefit society, or the developer is subject to the requirements of chapter 175 and any rules adopted by the commissioner of insurance.

(h) (1) a bank, out-of-state bank, credit union chartered by the state of Massachusetts, federal credit union, out-of-state credit union, or any affiliate or subsidiary thereof, is in full compliance with this chapter if the bank, out-of-state bank, credit union chartered by the state of Massachusetts, federal credit union, out-of-state credit union, or affiliate or subsidiary is subject to examination by a state or federal prudential regulator under any published guidance or regulations that apply to the use of high-risk artificial intelligence systems and the guidance or regulations:

(i) impose requirements that are substantially equivalent to or more stringent than the requirements imposed in this chapter; and

(ii) at a minimum, require the bank, out-of-state bank, credit union chartered by the state of Massachusetts, federal credit union, out-of-state credit union, or affiliate or subsidiary to:

(A) regularly audit the bank's, out-of-state bank's, credit union chartered by the state of Massachusetts', federal credit union's, out-of-state credit union's, or affiliate's or subsidiary's use of high-risk artificial intelligence systems for compliance with state and federal anti-discrimination laws and regulations applicable to the bank, out-of-state bank, credit union chartered by the state of Massachusetts federal credit union, out-of-state credit union, or affiliate or subsidiary; and

(B) mitigate any algorithmic discrimination caused by the use of a high-risk artificial intelligence system or any risk of algorithmic discrimination that is reasonably foreseeable as a result of the use of a high-risk artificial intelligence system.

(2) as used in this subsection (8):

(i) "Affiliate" has the meaning set forth in chapter 156D.

(ii) "Bank" has the meaning set forth in chapter 167.

(iii) "Credit union" has the meaning set forth in chapter 167.

(iv) "Out-of-state bank" has the meaning set forth in chapter 167.

(i) if a developer, a deployer, or other person engages in an action pursuant to an exemption set forth in this section, the developer, deployer, or other person bears the burden of demonstrating that the action qualifies for the exemption.

Section 6. Enforcement by attorney general

(a) the attorney general has exclusive authority to enforce this chapter.

(b) except as provided in subsection (c) of this section, a violation of the requirements established in this chapter constitutes an unfair trade practice pursuant to chapter 93A.

(c) in any action commenced by the attorney general to enforce this chapter, it is an affirmative that the developer, deployer, or other person:

(1) discovers and cures a violation of this this chapter 93 as a result of:

(i) feedback that the developer, deployer, or other person encourages deployers or users to provide to the developer, deployer, or other person;

(ii) adversarial testing or red teaming, as those terms are defined or used by the national institute of standards and technology; or

(iii) an internal review process; and

(2) is otherwise in compliance with:

(i) the latest version of the "Artificial intelligence risk management framework" published by the national institute of standards and technology in the United States Department of Commerce and Standard ISO/IEC 42001 of the International Organization for Standardization;

(ii) another nationally or internationally recognized risk management framework for artificial intelligence systems, if the standards are substantially equivalent to or more stringent than the requirements of this chapter; or

(iii) any risk management framework for artificial intelligence systems that the attorney general, in the attorney general's discretion, may designate and, if designated, shall publicly disseminate.

(d) a developer, a deployer, or other person bears the burden of demonstrating to the attorney general that the requirements established in subsection (3) of this section have been satisfied.

(e) nothing in this chapter, including the enforcement authority granted to the attorney general under this section, preempts or otherwise affects any right, claim, remedy, presumption, or defense available at law or in equity. A rebuttable presumption or affirmative defense established under this chapter applies only to an enforcement action brought by the attorney general pursuant to this section and does not apply to any right, claim, remedy, presumption, or defense available at law or in equity.

(f) this chapter does not provide the basis for, and is not subject to, a private right of action for violations of this chapter or any other law.

Section 7. Rules

(a) the attorney general may promulgate rules as necessary for the purpose of implementing and enforcing this chapter, including:

(1) the documentation and requirements for developers pursuant to section 2 (b);

(2) the contents of and requirements for the notices and disclosures required by sections 2 (c) and (g); 3 (d), (e), (g), and (i); and 4;

(3) the content and requirements of the risk management policy and program required by section 3 (b);

(4) the content and requirements of the impact assessments required by section 3 (c);

(5) the requirements for the rebuttable presumptions set forth in sections 2 and 3; and

(6) the requirements for the affirmative defense set forth in section 6 (c), including the process by which the attorney general will recognize any other nationally or internationally recognized risk management framework for artificial intelligence systems.

SECTION 2: This law shall take effect no later than 6 months after the passage of this bill.