STATE OF NEW YORK

1169--A

2025-2026 Regular Sessions

IN SENATE

January 8, 2025

Introduced by Sens. GONZALEZ, BAILEY, BRISPORT, BYNOE, CLEARE, FERNANDEZ, HINCHEY, JACKSON, LIU, MAY, PERSAUD, RIVERA, SALAZAR, SANDERS, WEBB -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the civil rights law and the executive law, in relation to the use of artificial intelligence systems

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "New York artificial intelligence act (New York AI act)".

§ 2. Legislative findings and intent. The legislature finds and declares the following:

(a) A revolution in artificial intelligence (AI) has advanced to the point that comprehensive regulations must be enacted to protect New Yorkers.

(b) Artificial intelligence is already an integral part of New Yorkers' daily lives. In the private sector, AI is currently in use in areas such as education, health care, employment, insurance, credit scoring, public safety, retail, banking and financial services, media, and more with little transparency or oversight. A growing body of research shows that AI systems that are deployed without adequate testing, sufficient oversight and robust guardrails can harm consumers and deny historically disadvantaged groups the full measure of their civil rights and liberties, thereby further entrenching inequalities. The legislature must act to ensure that all uses of AI, especially those that affect important life chances, are free from harmful biases, protect our privacy, and work for the public good.

(c) Safe innovation must remain a priority for the state. New York state is home to thousands of technology start-ups, many of which exper-

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD04409-02-5

iment with new applications of AI and which have the potential to find new ways to employ technology at the service of New Yorkers. The goal of the legislature is to encourage safe innovation in the AI sector by providing clear guidance for AI development, testing, and validation both before a product is launched and throughout the product's life cycle.

(d) New York must establish that the burden of responsibility of proving that AI products do not cause harm to New Yorkers will be shouldered by the developers and deployers of AI. While government and civil society must act to audit and enforce human rights laws around the use of AI, the companies employing and profiting from the use of AI must lead in ensuring that their products are free from algorithmic discrimination.

(e) Close collaboration and communication between New York state and industry partners is key to ensuring that innovation can occur with safeguards to protect all New Yorkers. This legislation will ensure that lines of communication exist and that there is clear statutory authority to investigate and prosecute entities that break the law.

(f) As new forms of AI are developed beyond what is currently technologically feasible, the goal of the legislature is to use this section as a guiding light for future regulations.

(g) Lastly, it is in the interest of all New Yorkers that certain uses of AI that infringe on fundamental rights, deepen structural inequality, or that result in unequal access to services shall be banned.

§ 3. The civil rights law is amended by adding a new article 8-A to read as follows:

ARTICLE 8-A

PROTECTIONS REGARDING USE OF ARTIFICIAL INTELLIGENCE

Section 85. Definitions.
86. Unlawful discriminatory practices.
86-a. Deployer and developer obligations.
86-b. Whistleblower protections.
87. Audits.
88. High-risk AI system reporting requirements.
89. Risk management policy and program.
89-a. Social scoring AI systems prohibited.
89-b. Developer safe harbor.
89-c. Enforcement.
89-d. Severability.

§ 85. Definitions. The following terms shall have the following meanings:

1. "Algorithmic discrimination" means any condition in which the use of an AI system contributes to unjustified differential treatment or impacts, disfavoring people based on their actual or perceived age, race, ethnicity, creed, religion, color, national origin, citizenship or immigration status, sexual orientation, gender identity, gender expression, military status, sex, disability, predisposing genetic characteristics, familial status, marital status, pregnancy, pregnancy outcomes, disability, height, weight, reproductive health care or autonomy, status as a victim of domestic violence or other classification protected under state or federal laws. Algorithmic discrimination shall not include:

(a) a developer's or deployer's testing of their own AI system to identify, mitigate, and prevent discriminatory bias;

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

(c) 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. section 2000a(e), as amended.

2. "Artificial intelligence system" or "AI system" means a machine-based system or combination of systems, that for explicit and implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Artificial intelligence system shall not include:

(a) any system that (i) is used by a business entity solely for internal purposes and (ii) is not used as a substantial factor in a consequential decision; or

(b) any software used primarily for basic computerized processes, such as anti-malware, anti-virus, auto-correct functions, calculators, databases, data storage, electronic communications, firewall, internet domain registration, internet website loading, networking, spam and robocall-filtering, spellcheck tools, spreadsheets, web caching, web hosting, or any tool that relates only to internal management affairs such as ordering office supplies or processing payments, and that do not materially affect the rights, liberties, benefits, safety or welfare of any individual within the state.

3. "Auditor" shall refer to an independent entity including but not limited to an individual, non-profit, firm, corporation, partnership, cooperative, association, academic institution, or group affiliated with an academic institution, commissioned to perform an audit.

4. "Consequential decision" means a decision or judgment that has a material, legal or similarly significant effect on an individual's access to, or the cost, terms, or availability of, any of the following:

(a) Employment, workers' management, or self-employment, including, but not limited to, all of the following:

(i) Pay or promotion; and

(ii) Hiring or termination.

(b) Education and vocational training, including, but not limited to, all of the following:

(i) Accreditation;

(ii) Certification;

(iii) Admissions; and

(iv) Financial aid or scholarships.

(c) Housing or lodging, including rental or short-term housing or lodging.

(d) Family planning, including adoption services or reproductive services, as well as assessments related to child protective services.

(e) Health care or health insurance, including mental health care, dental, or vision.

(f) Financial services, including a financial service provided by a mortgage company, mortgage broker, or creditor.

(g) Law enforcement activities, including the allocation of law enforcement personnel or assets, the enforcement of laws, maintaining public order, or managing public safety.

(h) Legal services.

5. "Deployer" means any person, partnership, association or corporation that offers or uses an AI system for commerce in the state of New York, or provides an AI system for use by the general public in the state of New York. A deployer shall not include any natural person

using an AI system for personal use. A developer may also be considered a deployer if its actions satisfy this definition.

6. "Developer" means a person, partnership, or corporation that designs, codes, or produces an AI system, or creates a substantial change with respect to an AI system, whether for its own use in the state of New York or for use by a third party in the state of New York. A deployer may also be considered a developer if its actions satisfy this definition.

7. "Employee" means an individual who performs services for and under the control and direction of an employer for wages or other remuneration, including former employees, or natural persons employed as independent contractors to carry out work in furtherance of an employer's business enterprise who are not themselves employers.

8. "Employer" means any person, firm, partnership, institution, corporation, or association that employs one or more employees.

9. "End user" means any individual or group of individuals that:

(a) is the subject of a consequential decision made entirely by or with the assistance of an AI system; or

(b) interacts, directly or indirectly, with the relevant AI system on behalf of an individual or group that is the subject of a consequential decision made entirely by or with the assistance of an AI system.

10. "High-risk AI system" means any AI system that, when deployed: (a) is a substantial factor in making a consequential decision; or (b) will have a material impact on the statutory or constitutional rights, civil liberties, safety, or welfare of an individual in the state.

11. "Risk management policy and program" means the risk management policy and program created pursuant to section eighty-nine of this article.

12. "Substantial change" means any new version, new release, or any other update to an AI system that results in significant changes to such AI system's appropriate use cases, key functionality, or expected outcomes.

13. "Substantial factor" means a factor that is (a) material in making a consequential decision, or (b) is capable of altering the outcome of a consequential decision.

§ 86. Unlawful discriminatory practices. It shall be an unlawful discriminatory practice for a developer or deployer to fail to comply with the duties under this section.

1. A developer or deployer shall take reasonable care to prevent foreseeable risk of algorithmic discrimination that is a consequence of the use, sale, or sharing of a high-risk AI system or a product featuring a high-risk AI system.

2. Any developer or deployer that uses, sells, or shares a high-risk AI system shall have completed an independent audit, pursuant to section eighty-seven of this article, confirming that the developer or deployer has taken reasonable care to prevent foreseeable risk of algorithmic discrimination with respect to such high-risk AI system.

§ 86-a. Deployer and developer obligations. 1. (a) Any deployer that employs a high-risk AI system for a consequential decision shall comply with the following requirements; provided, however, that where there is an urgent necessity for a decision to be made to confer a benefit to the end user, including, but not limited to, social benefits, housing access, or dispensing of emergency funds, and compliance with this section would cause imminent detriment to the welfare of the end user, such obligation shall be considered waived; provided further, that noth-

ing in this section shall be construed to waive a natural person's option to request human review of the decision:

(i) inform the end user at least five business days prior to the use of such system for the making of a consequential decision in clear, conspicuous, and consumer-friendly terms, made available in each of the languages in which the company offers its end services, that AI systems will be used to make a decision or to assist in making a decision; and

(ii) allow sufficient time and opportunity in a clear, conspicuous, and consumer-friendly manner for the consumer to opt-out of the automated consequential decision process and for the decision to be made by a human representative. A consumer may not be punished or face any other adverse action for opting out of a decision by an AI system and the deployer shall render a decision to the consumer within forty-five days.

(b) If a deployer employs a high-risk AI system for a consequential decision to determine whether to or on what terms to confer a benefit on an end user, the deployer shall offer the end user the option to waive their right to advance notice of five business days under this subdivision.

(c) If the end user clearly and affirmatively waives their right to five business days' notice, the deployer shall then inform the end user as early as practicable before the making of the consequential decision in clear, conspicuous, and consumer-friendly terms, made available in each of the languages in which the company offers its end services, that AI systems will be used to make a decision or to assist in making a decision. The deployer shall allow sufficient time and opportunity in a clear, conspicuous, and consumer-friendly manner for the consumer to opt-out of the automated process and for the decision to be made by a human representative. A consumer may not be punished or face any other adverse action for opting out of a decision by an AI system and the deployer shall render a decision to the consumer within forty-five days.

(d) An end user shall be entitled to no more than one opt-out with respect to the same consequential decision within a six-month period.

2. (a) Any deployer that employs a high-risk AI system for a consequential decision shall inform the end user within five days in a clear, conspicuous and consumer-friendly manner if a high-risk AI system has been used to make a consequential decision. The deployer shall then provide and explain a process for the end user to appeal the decision, which shall at minimum allow the end user to (i) formally contest the decision, (ii) provide information to support their position, and (iii) obtain meaningful human review of the decision. A deployer shall respond to an end user's appeal within forty-five days of receipt of the appeal. That period may be extended once by forty-five additional days where reasonably necessary, taking into account the complexity and number of appeals. The deployer shall inform the end user of any such extension within forty-five days of receipt of the appeal, together with the reasons for the delay.

(b) An end user shall be entitled to no more than one appeal with respect to the same consequential decision in a six-month period.

3. The deployer or developer of a high-risk AI system is legally responsible for quality and accuracy of all consequential decisions made, including any bias or algorithmic discrimination resulting from the operation of the AI system on their behalf.

4. The rights and obligations under this section may not be waived by any person, partnership, association or corporation.

5. With respect to a single consequential decision, an end user may not exercise both its right to opt-out of a consequential decision under

subdivision one of this section and its right to appeal a consequential decision under subdivision two of this section.

§ 86-b. Whistleblower protections. 1. Developers and/or deployers of high-risk AI systems shall not:

(a) prevent any of their employees from disclosing information to the attorney general, including through terms and conditions of employment or seeking to enforce terms and conditions of employment, if the employee has reasonable cause to believe the information indicates a violation of this article; or

(b) retaliate against an employee for disclosing information to the attorney general pursuant to this section.

2. An employee harmed by a violation of this article may petition a court for appropriate relief as provided in subdivision five of section seven hundred forty of the labor law.

3. Developers and deployers of high-risk AI systems shall provide a clear notice to all of their employees working on such AI systems of their rights and responsibilities under this article, including the right of employees of contractors and subcontractors to use the developer's internal process for making protected disclosures pursuant to subdivision four of this section. A developer or deployer is presumed to be in compliance with the requirements of this subdivision if the developer or deployer does either of the following:

(a) at all times post and display within all workplaces maintained by the developer or deployer a notice to all employees of their rights and responsibilities under this article, ensure that all new employees receive equivalent notice, and ensure that employees who work remotely periodically receive an equivalent notice; or

(b) no less frequently than once every year, provide written notice to all employees of their rights and responsibilities under this article and ensure that the notice is received and acknowledged by all of those employees.

4. Each developer and deployer shall provide a reasonable internal process through which an employee may anonymously disclose information to the developer or deployer if the employee believes in good faith that the information indicates that the developer or deployer has violated any provision of this article or any other law, or has made false or materially misleading statements related to its risk management policy and program, or failed to disclose known risks to employees, including, at a minimum, a monthly update to the person who made the disclosure regarding the status of the developer's or deployer's investigation of the disclosure and the actions taken by the developer or deployer in response to the disclosure.

5. This section does not limit protections provided to employees under section seven hundred forty of the labor law.

§ 87. Audits. 1. Developers of high-risk AI systems shall cause to be conducted third-party audits in accordance with this section.

(a) A developer of a high-risk AI system shall complete at least:

(i) a first audit within six months after completion of development of the high-risk AI system and the initial offering of the high-risk AI system to a deployer for deployment or, if the developer is first deployer to deploy the high-risk AI system, after initial deployment; and

(ii) one audit every one year following the submission of the first audit.

(b) A developer audit under this section shall include:

(i) an evaluation and determination of whether the developer has taken reasonable care to prevent foreseeable risk of algorithmic discrimination with respect to such high-risk AI system; and

(ii) an evaluation of the developer's documented risk management policy and program required under section eighty-nine of this article for conformity with subdivision one of such section eighty-nine.

2. Deployers of high-risk AI systems shall cause to be conducted third-party audits in accordance with this section.

(a) A deployer of a high-risk AI system shall complete at least:

(i) a first audit within six months after initial deployment;

(ii) a second audit within one year following the submission of the first audit; and

(iii) one audit every two years following the submission of the second audit.

(b) A deployer audit under this section shall include:

(i) an evaluation and determination of whether the deployer has taken reasonable care to prevent foreseeable risk of algorithmic discrimination with respect to such high-risk AI system;

(ii) an evaluation of system accuracy and reliability with respect to such high-risk AI system's deployer-intended and actual use cases; and

(iii) an evaluation of the deployer's documented risk management policy and program required under section eighty-nine of this article for conformity with subdivision one of such section eighty-nine.

3. A deployer or developer may hire more than one auditor to fulfill the requirements of this section.

4. At the attorney general's discretion, the attorney general may:

(a) promulgate further rules as necessary to ensure that audits under this section assess whether or not AI systems produce algorithmic discrimination and otherwise comply with the provisions of this article; and

(b) recommend an updated AI system auditing framework to the legislature, where such recommendations are based on a standard or framework (i) designed to evaluate the risks of AI systems, and (ii) that is nationally or internationally recognized and consensus-driven, including but not limited to a relevant framework or standard created by the International Standards Organization.

5. The independent auditor shall have complete and unredacted copies of all reports previously filed by the deployer or developer under section eighty-eight of this article.

6. An audit conducted under this section may be completed in part, but shall not be completed entirely, with the assistance of an AI system.

(a) Acceptable auditor uses of an AI system include, but are not limited to:

(i) use of an audited high-risk AI system in a controlled environment without impacts on end users for system testing purposes; or

(ii) detecting patterns in the behavior of an audited AI system.

(b) An auditor shall not:

(i) use a different high-risk AI system that is not the subject of an audit to complete an audit; or

(ii) use an AI system to draft an audit under this section without meaningful human review and oversight.

7. (a) An auditor shall be an independent entity including but not limited to an individual, non-profit, firm, corporation, partnership, cooperative, or association.

(b) For the purposes of this article, no auditor may be commissioned by a developer or deployer of a high-risk AI system if such entity:

(i) has already been commissioned to provide any auditing or non-auditing service, including but not limited to financial auditing, cybersecurity auditing, or consulting services of any type, to the commissioning company in the past twelve months; or

(ii) is, will be, or plans to be engaged in the business of developing or deploying an AI system that can compete commercially with such developer's or deployer's high-risk AI system in the five years following an audit.

(c) Fees paid to auditors may not be contingent on the result of the audit and the commissioning company shall not provide any incentives or bonuses for a positive audit result.

8. The attorney general may promulgate further rules to ensure (a) the independence of auditors under this section, and (b) that teams conducting audits incorporate feedback from communities that may foreseeably be the subject of algorithmic discrimination with respect to the AI system being audited.

9. If a developer or deployer has an audit completed for the purpose of complying with another applicable federal, state, or local law or regulation, and the audit otherwise satisfies all other requirements of this section, such audit shall be deemed to satisfy the requirements of this section.

§ 88. High-risk AI system reporting requirements. 1. Every developer and deployer of a high-risk AI system shall comply with the reporting requirements of this section.

2. Together with each report required to be filed under this section, every developer and deployer shall file with the attorney general a copy of the last completed independent audit required by this article.

3. Developers of high-risk AI systems shall complete and file with the attorney general reports in accordance with this subdivision.

(a) A developer of a high-risk AI system shall complete and file with the attorney general at least:

(i) a first report within six months after completion of development of the high-risk AI system and the initial offering of the high-risk AI system to a deployer for deployment or, if the developer is first deployer to deploy the high-risk AI system, after initial deployment;

(ii) one report annually following the submission of the first report; and

(iii) one report within six months of any substantial change to the high-risk AI system.

(b) A developer report under this section shall include:

(i) a description of the system including:

(A) the uses of the high-risk AI system that the developer intends; and

(B) any explicitly unintended or disallowed uses of the high-risk AI system;

(ii) an overview of how the high-risk AI system was developed;

(iii) an overview of the high-risk AI system's training data; and

(iv) any other information necessary to allow a deployer to:

(A) understand the outputs and monitor the system for compliance with this article; and

(B) fulfill its duties under this article.

4. Deployers of high-risk AI systems shall complete and file with the attorney general reports in accordance with this subdivision.

(a) A deployer of a high-risk AI system shall complete and file with the attorney general at least:

(i) a first report within six months after initial deployment;

(ii) a second report within one year following the completion and filing of the first report;

(iii) one report every two years following the completion and filing of the second report; and

(iv) one report within six months of any substantial change to the high-risk AI system.

(b) A deployer report under this section shall include:

(i) a description of the system including:

(A) the deployer's actual, intended, or planned uses of the high-risk AI system with respect to consequential decisions; and

(B) whether the deployer is using the high-risk AI system for any developer unintended or disallowed uses; and

(ii) an impact assessment including:

(A) whether the high-risk AI system poses a risk of algorithmic discrimination and the steps taken to address the risk of algorithmic discrimination;

(B) if the high-risk AI system is or will be monetized, how it is or is planned to be monetized; and

(C) an evaluation of the costs and benefits to consumers and other end users.

(c) A deployer that is also a developer and is required to submit reports under subdivision three of this section may submit a single joint report provided it contains the information required in this subdivision.

5. The attorney general shall:

(a) promulgate rules for a process whereby developers and deployers may request redaction of portions of reports required under this section to ensure that they are not required to disclose sensitive and protected information; and

(b) maintain an online database that is accessible to the general public with reports, redacted in accordance with this subdivision, and audits required by this article, which database shall be updated biannually.

6. For high-risk AI systems which are already in deployment at the time of the effective date of this article, developers and deployers shall have eighteen months from such effective date to complete and file the first report and associated independent audit required by this article.

(a) Each developer of a high-risk AI system shall thereafter file at least one report annually following the submission of the first report under this subdivision.

(b) Each deployer of a high-risk AI system shall thereafter file at least one report every two years following the submission of the first report under this subdivision.

§ 89. Risk management policy and program. 1. Each developer or deployer of high-risk AI systems shall plan, document, and implement a risk management policy and program to govern development or deployment, as applicable, of such high-risk AI system. The risk management policy and program shall 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 covered under subdivision one of section eighty-six of this article. The risk management policy and program shall be an iterative process planned, implemented, and regularly and systematically reviewed and updated over the life cycle of a high-risk AI system, requiring regular, systematic review and updates, including updates to documentation. A

risk management policy and program implemented and maintained pursuant to this section shall be reasonable considering:

(a) The guidance and standards set forth in:

(i) version 1.0 of the "Artificial Intelligence Risk Management Framework" published by the National Institute of Standards and Technology in the United States department of commerce, or

(ii) another substantially equivalent framework selected at the discretion of the attorney general, if such framework was designed to manage risks associated with AI systems, is nationally or internationally recognized and consensus-driven, and is at least as stringent as version 1.0 of the "Artificial Intelligence Risk Management Framework" published by the National Institute of Standards and Technology;

(b) The size and complexity of the developer or deployer;

(c) The nature, scope, and intended uses of the high-risk AI system developed or deployed; and

(d) The sensitivity and volume of data processed in connection with the high-risk AI system.

2. A risk management policy and program implemented pursuant to subdivision one of this section may cover multiple high-risk AI systems developed by the same developer or deployed by the same deployer if sufficient.

3. The attorney general may require a developer or a deployer to disclose the risk management policy and program implemented pursuant to subdivision one of this section in a form and manner prescribed by the attorney general. The attorney general may evaluate the risk management policy and program to ensure compliance with this section.

§ 89-a. Social scoring AI systems prohibited. No person, partnership, association or corporation shall develop, deploy, use, or sell an AI system which evaluates or classifies the trustworthiness of natural persons over a certain period of time based on their social behavior or known or predicted personal or personality characteristics, with the social score leading to any of the following:

1. differential treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

2. differential treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behavior or its gravity; or

3. the infringement of any right guaranteed under the United States constitution, the New York constitution, or state or federal law.

§ 89-b. Developer safe harbor. A developer may be exempt from its duties and obligations under sections eighty-six, eighty-six-a, eighty-six-b, eighty-seven, eighty-eight, and eighty-nine of this article if such developer:

1. receives a written and signed contractual agreement from each deployer authorized to use the artificial intelligence system developed by such developer, including the developer if they are also a deployer, that such artificial intelligence system will not be used as a high-risk AI system;

2. implements reasonable technical safeguards designed to prevent or detect high-risk AI system use cases or otherwise demonstrates reasonable steps taken to ensure that any unauthorized deployments of its AI systems are not being used as a high-risk AI system;

3. prominently displays on its website, in marketing materials, and in all licensing agreements offered to prospective deployers of its AI system that the AI system cannot be used as a high-risk AI system; and

4. maintains records of deployer agreements for a period of not less than five years.

§ 89-c. Enforcement. 1. Whenever there shall be a violation of section eighty-six-a, eighty-six-b, eighty-seven, eighty-eight, eighty-nine, or eighty-nine-a of this article, an application may be made by the attorney general in the name of the people of the state of New York, to the supreme court having jurisdiction to issue an injunction, and upon notice to the respondent of not less than ten days, to enjoin and restrain the continuance of such violation; and if it shall appear to the satisfaction of the court that the respondent has, in fact, violated this article, an injunction may be issued by the court, enjoining and restraining any further violations, without requiring proof that any person has, in fact, been injured or damaged thereby. In any such proceeding, the court may make allowances to the attorney general as provided in paragraph six of subdivision (a) of section eighty-three hundred three of the civil practice law and rules, and direct restitution. Whenever the court shall determine that a violation of this article has occurred, the court may impose a civil penalty of not more than twenty thousand dollars for each violation.

2. There shall be a private right of action by plenary proceeding for any person harmed by any violation of section eighty-six-a, eighty-six-b, eighty-seven, eighty-eight, eighty-nine, or eighty-nine-a of this article by any natural person or entity. The court shall award compensatory damages and legal fees to the prevailing party.

3. In evaluating any motion to dismiss a plenary proceeding commenced pursuant to subdivision two of this section, the court shall presume the specified AI system was created and/or operated in violation of a specified law or laws and that such violation caused the harm or harms alleged.

(a) A defendant can rebut presumptions made pursuant to this subdivision through clear and convincing evidence that the specified AI system did not cause the harm or harms alleged and/or did not violate the alleged law or laws. An algorithmic audit can be considered as evidence in rebutting such presumptions, but the mere existence of such an audit, without additional evidence, shall not be considered clear and convincing evidence.

(b) With respect to a violation of section eighty-six-a, eighty-six-b, eighty-seven, eighty-eight, or eighty-nine of this article, a developer can rebut presumptions made pursuant to this subdivision through clear and convincing evidence that it has complied with the duties under section eighty-nine-b of this article.

(c) Where such presumptions are not rebutted pursuant to this subdivision, the action shall not be dismissed.

(d) Where such presumptions are rebutted pursuant to this subdivision, a motion to dismiss an action shall be adjudicated without any consideration of this section.

4. The supreme court in the state shall have jurisdiction over any action, claim, or lawsuit to enforce the provisions of this article.

§ 89-d. Severability. If any clause, sentence, paragraph, subdivision, section or part of this article shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section, or part thereof directly involved in the controversy in which such judgment shall have been made.

§ 4. Section 296 of the executive law is amended by adding a new subdivision 23 to read as follows:

23. It shall be an unlawful discriminatory practice under this section for a deployer or a developer, as such terms are defined in section eighty-five of the civil rights law, to engage in an unlawful discriminatory practice under section eighty-six of the civil rights law.

§ 5. This act shall take effect one year after it shall have become a law; provided, however, that section 87 of article 8-A of the civil rights law as added by section three of this act shall take effect two years after it shall have become a law.