

LEGISLATURE OF NEBRASKA
ONE HUNDRED NINTH LEGISLATURE
FIRST SESSION

LEGISLATIVE BILL 642

Introduced by Bostar, 29.

Read first time January 22, 2025

Committee:

- 1 A BILL FOR AN ACT relating to discrimination; to adopt the Artificial
- 2 Intelligence Consumer Protection Act; and to provide severability.
- 3 Be it enacted by the people of the State of Nebraska,

1 **Section 1.** Sections 1 to 7 of this act shall be known and may be
2 cited as the Artificial Intelligence Consumer Protection Act.

3 **Sec. 2.** For purposes of the Artificial Intelligence Consumer
4 Protection Act:

5 (1)(a) Algorithmic discrimination means any use of an artificial
6 intelligence system that violates state or federal anti-discrimination
7 laws, including federal statutes prohibiting discrimination on the basis
8 of citizenship status, color, disability, national origin, race, or sex,
9 or any other classification protected under the laws of this state or
10 federal law; and

11 (b) Algorithmic discrimination does not include:

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

14 (A) The developer's or deployer's self-testing to identify,
15 mitigate, or prevent discrimination or otherwise ensure compliance with
16 state and federal law; or

17 (B) Expanding an applicant, customer, or participant pool to
18 increase diversity or redress historical discrimination; or

19 (ii) An act or omission by or on behalf of a private club or other
20 establishment that is not in fact open to the public, pursuant to the
21 federal Civil Rights Act of 1964, 42 U.S.C. 2000a(e), as such section
22 existed on January 1, 2025;

23 (2) Artificial intelligence system means any machine-based system
24 that, for any explicit or implicit objective, infers from the inputs the
25 system receives how to generate outputs, including content, decisions,
26 predictions, or recommendations, that can influence physical or virtual
27 environments;

28 (3) Consequential decision means a decision that has a material
29 legal or similarly significant effect on the provision or denial to any
30 consumer of any, or the cost or terms of any:

31 (a) Education enrollment or an education opportunity;

1 (b) Employment;

2 (c) Lending decision;

3 (d) Essential government service;

4 (e) Health care services;

5 (f) Housing;

6 (g) Insurance;

7 (h) Legal service; or

8 (i) Pardon, parole, probation, or release decision;

9 (4) Consumer means any individual who is a resident of this state;

10 (5) Deploy means to use a high-risk artificial intelligence system;

11 (6) Deployer means a person doing business in this state that
12 deploys a high-risk artificial intelligence system in this state;

13 (7) Developer means a person doing business in this state that
14 develops or intentionally and substantially modifies a high-risk
15 artificial intelligence system in this state;

16 (8) Health care services has the same meaning as in 42 U.S.C. 234(d)
17 (2), as such section existed on January 1, 2025;

18 (9)(a) High-risk artificial intelligence system means any artificial
19 intelligence system that, when deployed, makes a consequential decision
20 without human review or intervention; and

21 (b) High-risk artificial intelligence system does not include:

22 (i) Any artificial intelligence system if the artificial
23 intelligence system is intended to:

24 (A) Perform a narrow procedural task;

25 (B) Improve the result of a previously completed human activity;

26 (C) Perform a preparatory task to an assessment that is relevant to
27 a consequential decision; or

28 (D) Detect decisionmaking patterns or deviations from preexisting
29 decisionmaking patterns and is not intended to replace or influence a
30 previously completed human assessment without sufficient human review;
31 and

1 (ii) Any of the following technology:

2 (A) Antifraud technology;

3 (B) Antimalware;

4 (C) Antivirus;

5 (D) Artificial intelligence-enabled video game;

6 (E) Calculator;

7 (F) Cybersecurity;

8 (G) Database;

9 (H) Data storage;

10 (I) Firewall;

11 (J) Internet domain registration;

12 (K) Internet website loading;

13 (L) Networking;

14 (M) Spam-filtering;

15 (N) Robocall-filtering;

16 (O) Spell-checking;

17 (P) Spreadsheet;

18 (Q) Web caching;

19 (R) Web hosting or any similar technology; or

20 (S) Technology that:

21 (I) Communicates with any consumer in natural language for the
22 purpose of providing such consumer with information, making any referral
23 or recommendation, or answering any question; and

24 (II) Is subject to an acceptable use policy that prohibits
25 generating content that is unlawful or harmful;

26 (10) Insurer means any person engaged as principal, indemnitor,
27 surety, or contractor in the business of making contracts of insurance;

28 (11)(a) Intentional and substantial modification means a deliberate
29 and material change made to an artificial intelligence system that
30 materially increases the known risk of algorithmic discrimination; and

31 (b) Intentional and substantial modification does not include any

1 change made to any high-risk artificial intelligence system, or the
2 performance of any high-risk artificial intelligence system, if:

3 (i) The high-risk artificial intelligence system continues to learn
4 after the high-risk artificial intelligence system is:

5 (A) Offered, sold, leased, licensed, given, or otherwise made
6 available to a deployer; or

7 (B) Deployed;

8 (ii) The change is made to the high-risk artificial intelligence
9 system as a result of any learning described in subdivision (10)(b)(i) of
10 this section;

11 (iii) The change was predetermined by the deployer, or a third party
12 contracted by the deployer, when the deployer or third party completed an
13 initial impact assessment of such high-risk artificial intelligence
14 system pursuant to subsection (3) of section 4 of this act; and

15 (iv) The change is included in technical documentation for the high-
16 risk artificial intelligence system;

17 (12) Intentionally and substantially modifies means intentional and
18 substantial modification as defined in this section;

19 (13) Principal basis means the use of an output of a high-risk
20 artificial intelligence system to make a decision without:

21 (a) Human review, oversight, involvement, or intervention; or

22 (b) Meaningful consideration by a human;

23 (14) Red teaming means an exercise that is conducted to identify the
24 potential adverse behaviors or outcomes of an artificial intelligence
25 system, identify how such behaviors or outcomes occur, and stress test
26 the safeguards against such behaviors or outcomes;

27 (15)(a) Substantial factor means any factor that:

28 (i) Is the principal basis for making a consequential decision;

29 (ii) Is capable of altering the outcome of a consequential decision;

30 and

31 (iii) Is generated by an artificial intelligence system; and

1 (b) Substantial factor includes any use of any artificial
2 intelligence system to generate any content, decision, prediction, or
3 recommendation concerning any consumer that is used as a basis to make a
4 consequential decision concerning the consumer; and

5 (16) Trade secret has the same meaning as in section 87-502.

6 **Sec. 3.** (1)(a) On and after February 1, 2026, a developer of a
7 high-risk artificial intelligence system shall use reasonable care to
8 protect consumers from any known risks of algorithmic discrimination
9 arising from the intended and contracted uses of the high-risk artificial
10 intelligence system.

11 (b) In any enforcement action brought on or after February 1, 2026,
12 by the Attorney General pursuant to section 7 of this act, there is a
13 rebuttable presumption that a developer used reasonable care as required
14 under this section if the developer complied with this section.

15 (2) Except as otherwise provided in subsection (6) of this section,
16 on and after February 1, 2026, each developer of a high-risk artificial
17 intelligence system shall make available to the deployer or other
18 developer of the high-risk artificial intelligence system:

19 (a) A general statement describing the uses and known harmful or
20 inappropriate uses of the high-risk artificial intelligence system;

21 (b) Documentation disclosing:

22 (i) A high-level summary of the types of data used to train the
23 high-risk artificial intelligence system;

24 (ii) Each known limitation of the high-risk artificial intelligence
25 system, including each known or reasonably foreseeable risk of
26 algorithmic discrimination arising from the intended use of the high-risk
27 artificial intelligence system;

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

29 (iv) Any intended benefit and use of the high-risk artificial
30 intelligence system; and

31 (v) Information necessary to allow the deployer to comply with the

1 requirements of section 4 of this act;

2 (c) Documentation describing:

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

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

10 (iii) Intended outputs of the high-risk artificial intelligence
11 system;

12 (iv) The measures the developer has taken to mitigate known risks of
13 algorithmic discrimination that could arise from the deployment of the
14 high-risk artificial intelligence system; and

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

19 (d) Documentation that is reasonably necessary to assist the
20 deployer in understanding each output and monitor the performance of the
21 high-risk artificial intelligence system for each risk of algorithmic
22 discrimination.

23 (3)(a) Except as otherwise provided in subsection (6) of this
24 section, on or after February 1, 2026, a developer that offers, sells,
25 leases, licenses, gives, or otherwise makes any high-risk artificial
26 intelligence system available to a deployer or other developer shall to
27 the extent feasible make available to the deployer or other developer the
28 documentation and information necessary for the deployer or a third party
29 contracted by the deployer to complete an impact assessment pursuant to
30 subsection (3) of section 4 of this act. Such documentation and
31 information includes any model card or other impact assessment.

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

6 (4)(a) On and after February 1, 2026, a developer shall make a
7 statement summarizing the following available in a manner that is clear
8 and readily available in a public use case inventory:

9 (i) The types of high-risk artificial intelligence systems that the
10 developer has developed and currently makes available to a deployer or
11 other developer;

12 (ii) The types of high-risk artificial intelligence system that the
13 developer has intentionally and substantially modified and currently
14 makes available to a deployer or other developer; and

15 (iii) How the developer manages known risks of algorithmic
16 discrimination that could arise from the development or intentional and
17 substantial modification of the types of high-risk artificial
18 intelligence systems described in subdivisions (4)(a)(i) and (ii) of this
19 section.

20 (b) A developer shall update the statement described in subdivision
21 (4)(a) of this section:

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

23 (ii) No later than ninety days after the developer intentionally and
24 substantially modifies any high-risk artificial intelligence system
25 described in subdivision (4)(a)(ii) of this section.

26 (5)(a) On and after February 1, 2026, a developer of a high-risk
27 artificial intelligence system shall disclose to all known deployers or
28 other developers of the high-risk artificial intelligence system, each
29 known risk of algorithmic discrimination arising from any intended use of
30 the high-risk artificial intelligence system without unreasonable delay
31 after the date on which:

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

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

8 (b) The Attorney General shall prescribe the form and manner of the
9 disclosure described in subdivision (a) of this subsection.

10 (6) Nothing in subsections (2) through (5) of this section requires
11 a developer to disclose any:

12 (a) Trade secret;

13 (b) Information protected from disclosure by state or federal law;
14 or

15 (c) Information that would create a security risk to the developer.

16 (7)(a) On and after February 1, 2026, the Attorney General may
17 provide a written demand to any developer to disclose to the Attorney
18 General the statement or documentation described in subsection (2) of
19 this section if such a statement or documentation is relevant to an
20 investigation related to the developer conducted by the Attorney General.
21 Such statement or documentation shall be provided to the Attorney General
22 in a form and manner prescribed by the Attorney General.

23 (b) The Attorney General may evaluate such statement or
24 documentation, if it is relevant to an investigation conducted by the
25 Attorney General regarding a violation of the Artificial Intelligence
26 Consumer Protection Act, to ensure compliance with the Artificial
27 Intelligence Consumer Protection Act.

28 (c) In any disclosure pursuant to this subsection, any developer may
29 designate the statement or documentation as including proprietary
30 information or a trade secret.

31 (d) To the extent any such statement or documentation includes any

1 proprietary information or any trade secret, such statement or
2 documentation shall be exempt from disclosure.

3 (8) If a developer completes documentation for the purpose of
4 complying with another applicable law or regulation, such documentation
5 shall be deemed to satisfy this section if such documentation is
6 reasonably similar in scope and effect to the documentation that would
7 otherwise be completed pursuant to this section.

8 **Sec. 4.** (1)(a) On and after February 1, 2026, a deployer of any
9 high-risk artificial intelligence system shall use reasonable care to
10 protect consumers from each known risk of algorithmic discrimination.

11 (b) In any enforcement action brought on or after February 1, 2026,
12 by the Attorney General pursuant to section 7 of this act, there is a
13 rebuttable presumption that a deployer of a high-risk artificial
14 intelligence system used reasonable care as required under this section
15 if the deployer complied with this section.

16 (2)(a) Except as otherwise provided in subsection (6) of this
17 section, on and after February 1, 2026, a deployer of a high-risk
18 artificial intelligence system shall implement a risk management policy
19 and program to govern the deployer's deployment of the high-risk
20 artificial intelligence system. High-risk artificial intelligence systems
21 that are in conformity with the guidance and standards set forth in the
22 following as of January 1, 2025, shall be presumed to be in conformity
23 with this section:

24 (i) The Artificial Intelligence Risk Management Framework published
25 by the National Institute of Standards and Technology; or

26 (ii) The standard ISO/IEC 42001 of the International Organization
27 for Standardization.

28 (b) Any risk management policy and program implemented pursuant to
29 subdivision (a) of this subsection may cover multiple high-risk
30 artificial intelligence systems deployed by the deployer.

31 (3)(a) Except as otherwise provided in this subsection or subsection

1 (6) of this section:

2 (i) An impact assessment shall be completed for each high-risk
3 artificial intelligence system deployed on or after February 1, 2026.

4 Such impact assessment shall be completed by the deployer or by a third
5 party contracted by the deployer; and

6 (ii) On and after February 1, 2026, for each deployed high-risk
7 artificial intelligence system, a deployer or a third party contracted by
8 the deployer shall complete an impact assessment within ninety days after
9 any intentional and substantial modification to such high-risk artificial
10 intelligence system is made available.

11 (b) An impact assessment completed pursuant to this subsection shall
12 include to the extent reasonably known by or available to the deployer:

13 (i) A statement by the deployer disclosing:

14 (A) The purpose of the high-risk artificial intelligence system;

15 (B) Any intended-use case for the high-risk artificial intelligence
16 system;

17 (C) The deployment context of the high-risk artificial intelligence
18 system; and

19 (D) Any benefit afforded by the high-risk artificial intelligence
20 system;

21 (ii) An analysis of whether the deployment of the high-risk
22 artificial intelligence system poses any known risk of algorithmic
23 discrimination and, if so, the nature of the algorithmic discrimination
24 and the steps that have been taken to mitigate any such risk;

25 (iii) A high-level summary of the categories of data the high-risk
26 artificial intelligence system processes as inputs and the outputs the
27 high-risk artificial intelligence system produces;

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

31 (v) Any metric used to evaluate the performance and any known

1 limitation of the high-risk artificial intelligence system;

2 (vi) A description of any transparency measure taken concerning the
3 high-risk artificial intelligence system, including any measure taken to
4 disclose to a consumer when the high-risk artificial intelligence system
5 is in use; and

6 (vii) A description of each postdeployment monitoring and user
7 safeguard provided concerning the high-risk artificial intelligence
8 system, including the oversight, use, and learning process established by
9 the deployer to address any issue that arises from the deployment of the
10 high-risk artificial intelligence system.

11 (c) Any impact assessment completed pursuant to this subsection
12 following an intentional and substantial modification to a high-risk
13 artificial intelligence system on or after February 1, 2026, shall
14 include a statement that discloses the extent to which the high-risk
15 artificial intelligence system was used in a manner that was consistent
16 with or varied from any use of the high-risk artificial intelligence
17 system intended by the developer.

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

20 (e) Any impact assessment completed to comply with another
21 applicable law or regulation by a deployer or by a third party contracted
22 by the deployer shall satisfy this subsection if such impact assessment
23 is reasonably similar in scope and effect to the impact assessment that
24 would otherwise be completed pursuant to this subsection.

25 (f) A deployer shall maintain:

26 (i) The most recently completed impact assessment required under
27 this subsection for each high-risk artificial intelligence system of the
28 deployer;

29 (ii) Each record concerning each such impact assessment; and

30 (iii) For at least three years following the final deployment of
31 each high-risk artificial intelligence system, each prior impact

1 assessment, if any, and each record concerning such impact assessment.

2 (4)(a) On and after February 1, 2026, prior to deploying any high-
3 risk artificial intelligence system to make or be a substantial factor in
4 making any consequential decision concerning any consumer, the deployer
5 shall:

6 (i) Notify the consumer that the deployer has deployed a high-risk
7 artificial intelligence system to make or be a substantial factor in
8 making a consequential decision;

9 (ii) Provide to the consumer:

10 (A) A statement that discloses the purpose of the high-risk
11 artificial intelligence system and the nature of the consequential
12 decision;

13 (B) The contact information for the deployer;

14 (C) A description written in plain language that describes the high-
15 risk artificial intelligence system; and

16 (D) Instructions on how to access the statement described in
17 subdivision (5)(a) of this section; and

18 (iii) If applicable, provide information to the consumer regarding
19 the consumer's right to opt out of the processing of personal data
20 concerning the consumer for any purpose of profiling in furtherance of
21 decisions that produce legal or similarly significant effects concerning
22 the consumer under subdivision (2)(e)(iii) of section 87-1107.

23 (b) On and after February 1, 2026, for each high-risk artificial
24 intelligence system that makes or is a substantial factor in making any
25 consequential decision that is adverse to any consumer, the deployer of
26 such high-risk artificial intelligence system shall provide to such
27 consumer:

28 (i) A statement that discloses each principal reason for the
29 consequential decision, including:

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

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

3 (C) Each source of the data described in subdivision (b)(i)(B) of
4 this subsection;

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

8 (iii) An opportunity to appeal any adverse consequential decision
9 concerning the consumer arising from the deployment of the high-risk
10 artificial intelligence system unless providing the opportunity for
11 appeal is not in the best interest of the consumer, including instances
12 when any delay might pose a risk to the life or safety of such consumer.
13 Any such appeal shall allow for human review if technically feasible.

14 (c)(i) Except as provided in subdivision (c)(ii) of this subsection,
15 a deployer shall provide the notice, statement, contact information, and
16 description required under subdivisions (4)(a) and (b) of this section:

17 (A) Directly to the consumer;

18 (B) In plain language;

19 (C) In each language in which the deployer in the ordinary course of
20 business provides any contract, disclaimer, sale announcement, or other
21 information to any consumer; and

22 (D) In a format that is accessible to any consumer with any
23 disability.

24 (ii) If the deployer is unable to provide the notice, statement,
25 contact information, and description required under subdivisions (a) and
26 (b) of this subsection directly to the consumer, the deployer shall make
27 the notice, statement, contact information, and description available in
28 a manner that is reasonably calculated to ensure that the consumer
29 receives the notice, statement, contact information, and description.

30 (5)(a) Except as provided in subsection (6) of this section, on and
31 after February 1, 2026, a deployer shall make a statement with the

1 following information available in a manner that is clear and readily
2 available:

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

5 (ii) How the deployer manages known risks of algorithmic
6 discrimination that may arise from the deployment of the types of high-
7 risk artificial intelligence systems described in subdivision (a)(ii) of
8 this subsection; and

9 (iii) A description of the nature, source, and extent of the
10 information collected and used by the deployer.

11 (b) A deployer shall update the statement described in subdivision
12 (a) of this subsection at least once each year.

13 (6) Subsections (2), (3), and (5) of this section do not apply to a
14 deployer if when deploying a high-risk artificial intelligence system and
15 at all times while the high-risk artificial intelligence system is
16 deployed:

17 (a) The deployer:

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

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

21 (b) The high-risk artificial intelligence system:

22 (i) Is used for any intended use that is disclosed to the deployer
23 as required under subdivision (2)(a) of section 3 of this act; and

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

26 (c) The deployer makes available to consumers any impact assessment
27 that:

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

30 (ii) Includes information that is substantially similar to the
31 information in the impact assessment required under subdivision (3)(b) of

1 this section.

2 (7) Nothing in this section requires a deployer to disclose a trade
3 secret or information protected from disclosure by state or federal law.
4 To the extent that a deployer withholds information pursuant to this
5 subsection or subsection (5) of section 6 of this act, the deployer shall
6 notify the consumer and provide a basis for such withholding.

7 (8)(a) On and after February 1, 2026, in connection with an ongoing
8 investigation related to the deployer, the Attorney General may require
9 any deployer or third party contracted by a deployer to disclose any of
10 the following to the Attorney General no later than ninety days after
11 such request in a form and manner prescribed by the Attorney General:

12 (i) The risk management policy implemented pursuant to subsection
13 (2) of this section;

14 (ii) The impact assessment completed pursuant to subsection (3) of
15 this section; or

16 (iii) The records maintained pursuant to subdivision (3)(f) of this
17 section.

18 (b) If such risk management policy, impact assessment, or record is
19 relevant to an investigation conducted by the Attorney General regarding
20 a violation of the Artificial Intelligence Consumer Protection Act, the
21 Attorney General may evaluate the risk management policy, impact
22 assessment, or records disclosed pursuant to subdivision (a) of this
23 subsection to ensure compliance with the Artificial Intelligence Consumer
24 Protection Act.

25 (c) Any disclosure under this subsection shall not be a public
26 record subject to disclosure pursuant to sections 84-712 to 84-712.09.

27 (d) A deployer may designate any statement or documentation
28 disclosed under this subsection as including proprietary information or a
29 trade secret.

30 (9) If a deployer completes documentation for the purpose of
31 complying with another applicable law or regulation, such documentation

1 shall be deemed to satisfy this section if such documentation is
2 reasonably similar in scope and effect to the documentation that would
3 otherwise be completed pursuant to this section.

4 **Sec. 5.** (1) On and after February 1, 2026, and except as otherwise
5 provided in subsection (2) of this section, a deployer or other developer
6 that deploys, offers, sells, leases, licenses, gives, or otherwise makes
7 available any artificial intelligence system that is intended to interact
8 with any consumer shall include in the disclosure to each consumer who
9 interacts with such artificial intelligence system that the consumer is
10 interacting with an artificial intelligence system.

11 (2) Disclosure is not required under subsection (1) of this section
12 under any circumstance when it would be obvious to a reasonable person
13 that the person is interacting with an artificial intelligence system.

14 **Sec. 6.** (1) The Artificial Intelligence Consumer Protection Act
15 does not restrict the ability of any developer, deployer, or other person
16 to:

17 (a) Comply with federal, state, or municipal laws, ordinances, or
18 regulations;

19 (b) Comply with any civil, criminal, or regulatory inquiry,
20 investigation, subpoena, or summons by any federal, state, municipal, or
21 other governmental authority;

22 (c) Cooperate with any law enforcement agency concerning conduct or
23 activity that the developer, deployer, or other person reasonably and in
24 good faith believes may violate any federal, state, or municipal law,
25 ordinance, or regulation;

26 (d) Investigate, establish, exercise, prepare for, or defend any
27 legal claim;

28 (e) Take immediate action to protect any interest that is essential
29 for the life or physical safety of any consumer or another individual;

30 (f) By any means:

31 (i) Prevent, detect, protect against, or respond to any security

1 incident, identity theft, fraud, harassment, malicious or deceptive
2 activity, or illegal activity;

3 (ii) Investigate, report, or prosecute any person responsible for
4 any action described in subdivision (f)(i) of this subsection; or

5 (iii) Preserve the integrity or security of any system of the
6 developer, deployer, or other person;

7 (g) Engage in public or peer-reviewed scientific or statistical
8 research in the public interest that:

9 (i) Adheres to each applicable ethics or privacy law; and

10 (ii) Is conducted in accordance with 45 C.F.R. part 46, as such
11 section existed on January 1, 2025, or any relevant requirement
12 established by the federal Food and Drug Administration;

13 (h) Conduct any research, testing, or development activity regarding
14 any artificial intelligence system or model, other than testing conducted
15 under real-world conditions, before the artificial intelligence system or
16 model is placed on the market, deployed, or put into service; or

17 (i) Provide assistance complying with the Artificial Intelligence
18 Consumer Protection Act to any other developer, deployer, or person.

19 (2) The Artificial Intelligence Consumer Protection Act does not
20 restrict the ability of any developer, deployer, or other person to:

21 (a) Effectuate a product recall; or

22 (b) Identify and repair any technical error that impairs existing or
23 intended functionality of any artificial intelligence system.

24 (3) The Artificial Intelligence Consumer Protection Act does not
25 apply to any instance in which compliance with such act would violate any
26 evidentiary privilege under the laws of this state.

27 (4) The Artificial Intelligence Consumer Protection Act does not and
28 shall not be construed to impose any obligation on any developer,
29 deployer, or other person that adversely affects any right or freedom of
30 any person, including the rights of a person to freedom of speech or
31 freedom of the press.

1 (5) The Artificial Intelligence Consumer Protection Act does not
2 apply to any developer, deployer, or other person:

3 (a) If the developer, deployer, or other person develops, deploys,
4 puts into service, or intentionally and substantially modifies any high-
5 risk artificial intelligence system:

6 (i) That has been approved, authorized, certified, cleared,
7 developed, deployed, or granted by any federal agency acting within the
8 scope of authority of such federal agency; or

9 (ii) In compliance with standards established by any federal agency,
10 if the standards are substantially equivalent or more stringent than the
11 requirements of the Artificial Intelligence Consumer Protection Act;

12 (b) Conducting research to support an application:

13 (i) For approval or certification from any federal agency, federal
14 administration, or federal commission; or

15 (ii) That is subject to review by any federal agency, federal
16 administration, or federal commission;

17 (c) Performing work under or in connection with any contract with
18 the United States Department of Commerce, the United States Department of
19 Defense, or the National Aeronautics and Space Administration, unless
20 such work relates to any high-risk artificial intelligence system that is
21 used to make or is a substantial factor in making a decision concerning
22 employment or housing; or

23 (d) That is providing or facilitating any health care recommendation
24 that:

25 (i) Is generated by any artificial intelligence system; and

26 (ii) Includes a health care provider in the process to implement the
27 recommendation.

28 (6) The Artificial Intelligence Consumer Protection Act does not
29 apply to any artificial intelligence system that is acquired by or for
30 the federal government or any federal agency or department, unless the
31 artificial intelligence system is a high-risk artificial intelligence

1 system that is used to make or is a substantial factor in making a
2 decision concerning employment or housing.

3 (7) The Artificial Intelligence Consumer Protection Act does not
4 apply to any of the following that are subject to the Unfair Insurance
5 Trade Practices Act:

6 (a) Any insurer;

7 (b) Any fraternal benefit society as described in section 44-1072;
8 and

9 (c) Any developer of an artificial intelligence system used by an
10 insurer.

11 (8)(a) For purposes of this subsection:

12 (i) Affiliate has the same meaning as in section 8-916;

13 (ii) Bank has the same meaning as in section 8-909; and

14 (iii) Credit union has the same meaning as in section 21-1705.

15 (b) The Artificial Intelligence Consumer Protection Act does not
16 apply to any bank, credit union, affiliate or subsidiary of any bank or
17 credit union, or service provider that is subject to examination by any
18 state or federal prudential regulator under any published guidance or
19 regulations that apply to the use of high-risk artificial intelligence
20 systems and the guidance or regulations:

21 (i) Impose requirements that are substantially equivalent to or more
22 stringent than the requirements imposed in the Artificial Intelligence
23 Consumer Protection Act as determined by the Attorney General; and

24 (ii) At a minimum, require the bank, credit union, affiliate or
25 subsidiary of the bank or credit union, or service provider to:

26 (A) Regularly audit the use of any high-risk artificial intelligence
27 system by the bank, credit union, or affiliate or subsidiary of the bank
28 or credit union for compliance with state and federal antidiscrimination
29 laws and regulations applicable to the bank, credit union, affiliate or
30 subsidiary of the bank or credit union, or service provider; and

31 (B) Mitigate any algorithmic discrimination caused by the use of any

1 high-risk artificial intelligence system or any risk of algorithmic
2 discrimination that is a result of the use of any high-risk artificial
3 intelligence system.

4 (9) If any developer, deployer, or other person engages in any
5 action pursuant to an exemption set forth in this section, the developer,
6 deployer, or other person bears the burden of demonstrating that the
7 action qualifies for the exemption.

8 (10) This section does not apply to:

9 (a) Artificial intelligence systems, including their output,
10 specifically developed and put into service for the sole purpose of
11 scientific research and development;

12 (b) A regulated entity subject to the supervision and regulation of
13 the Federal Housing Finance Agency; or

14 (c) A creditor as defined by and subject to the federal Equal Credit
15 Opportunity Act, 15 U.S.C. 1691 et seq., or the regulations adopted
16 pursuant to such act.

17 **Sec. 7.** (1) The Attorney General has exclusive authority to enforce
18 the Artificial Intelligence Consumer Protection Act.

19 (2) Except as provided in subsection (5) of this section, the
20 Attorney General shall, prior to initiating any action for a violation of
21 the Artificial Intelligence Consumer Protection Act, issue a notice of
22 violation to the developer, deployer, or other person describing with
23 specificity the alleged violation and the actions that shall be taken by
24 the recipient of the notice to cure the violation. If the developer,
25 deployer, or other person fails to cure such violation not later than
26 ninety days after receipt of the notice of violation, the Attorney
27 General may bring an action under the Artificial Intelligence Consumer
28 Protection Act.

29 (3) In any action commenced by the Attorney General to enforce the
30 Artificial Intelligence Consumer Protection Act, it is an affirmative
31 defense that the developer, deployer, or other person:

1 (a) Discovers and cures a violation of the Artificial Intelligence
2 Consumer Protection Act as a result of:

3 (i) Feedback that the developer, deployer, or other person
4 encourages deployers or users to provide to the developer, deployer, or
5 other person;

6 (ii) Adversarial testing or red teaming; or

7 (iii) An internal review process; and

8 (b) Is otherwise in compliance with:

9 (i) The Artificial Intelligence Risk Management Framework published
10 by the National Institute of Standards and Technology and standard
11 ISO/IEC 42001 of the International Organization for Standardization, as
12 such framework and standard existed on January 1, 2025;

13 (ii) Another nationally or internationally recognized risk
14 management framework for artificial intelligence systems, if the
15 standards are substantially equivalent to or more stringent than the
16 requirements of the Artificial Intelligence Consumer Protection Act as
17 determined by the Attorney General; or

18 (iii) Any risk management framework for artificial intelligence
19 systems designated and publicly disseminated by the Attorney General.

20 (4) Any developer, deployer, or other person bears the burden of
21 demonstrating to the Attorney General that the requirements of subsection
22 (3) of this section have been satisfied.

23 (5)(a) The Artificial Intelligence Consumer Protection Act shall not
24 be construed to preempt or otherwise affect any right, claim, remedy,
25 presumption, or defense available at law or in equity.

26 (b) Any rebuttable presumption or affirmative defense under the
27 Artificial Intelligence Consumer Protection Act applies only to an
28 enforcement action brought by the Attorney General pursuant to this
29 section and shall not apply to any right, claim, remedy, presumption, or
30 defense available at law or in equity.

31 (6) The Artificial Intelligence Consumer Protection Act does not

1 provide the basis for and is not subject to any private right of action
2 for any violation of the Artificial Intelligence Consumer Protection Act
3 or any other law.

4 **Sec. 8.** If any section in this act or any part of any section is
5 declared invalid or unconstitutional, the declaration shall not affect
6 the validity or constitutionality of the remaining portions.