



104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

HB2838

Introduced 2/6/2025, by Rep. Dan Ugaste

SYNOPSIS AS INTRODUCED:

740 ILCS 14/10
740 ILCS 14/15
740 ILCS 14/20
740 ILCS 14/25

Amends the Biometric Information Privacy Act. Changes the definition of "biometric identifier". Defines "biometric lock", "biometric time clock", "person", and "security purpose". Waives certain requirements for collecting, capturing, or otherwise obtaining a person's or a customer's biometric identifier or biometric information under certain circumstances relating to security purposes. Provides that nothing in the Act shall be construed to apply to information captured by a biometric time clock or biometric lock that converts a person's biometric identifier or biometric information to a mathematical representation. Provides that any person aggrieved by a violation of this Act has a right of action in State court or federal court within one year from its occurrence. Requires the aggrieved person to provide the private entity 30 days a written entity alleging the specific provisions of the Act that have been violated. Provides the private entity 30 days to cure the noticed violation. Exempts a private entity if its employees are covered by a collective bargaining agreement that provides for different policies regarding the retention, collection, disclosure, and destruction of biometric information. Effective immediately.

LRB104 08099 JRC 18145 b

1 AN ACT concerning civil law.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 5. The Biometric Information Privacy Act is
5 amended by changing Sections 10, 15, 20, and 25 as follows:

6 (740 ILCS 14/10)

7 Sec. 10. Definitions. In this Act:

8 "Biometric identifier" means a retina or iris scan,
9 fingerprint, voiceprint, or scan of hand or face geometry.
10 Biometric identifiers do not include writing samples, written
11 signatures, photographs, human biological samples used for
12 valid scientific testing or screening, demographic data,
13 tattoo descriptions, or physical descriptions such as height,
14 weight, hair color, or eye color. Biometric identifiers do not
15 include donated organs, tissues, or parts as defined in the
16 Illinois Anatomical Gift Act or blood or serum stored on
17 behalf of recipients or potential recipients of living or
18 cadaveric transplants and obtained or stored by a federally
19 designated organ procurement agency. Biometric identifiers do
20 not include biological materials regulated under the Genetic
21 Information Privacy Act. Biometric identifiers do not include
22 information captured from a patient in a health care setting
23 or information collected, used, or stored for health care

1 treatment, payment, or operations under the federal Health
2 Insurance Portability and Accountability Act of 1996.
3 Biometric identifiers do not include an X-ray, roentgen
4 process, computed tomography, MRI, PET scan, mammography, or
5 other image or film of the human anatomy used to diagnose,
6 prognose, or treat an illness or other medical condition or to
7 further validate scientific testing or screening. "Biometric
8 identifier" does not include (i) information captured and
9 converted to a mathematical representation, including, but not
10 limited to, a numeric string or similar method that cannot be
11 used to recreate the biometric identifier or (ii) information
12 that cannot reasonably be used to identify an individual.

13 "Biometric information" means any information, regardless
14 of how it is captured, converted, stored, or shared, based on
15 an individual's biometric identifier used to identify an
16 individual. Biometric information does not include information
17 derived from items or procedures excluded under the definition
18 of biometric identifiers.

19 "Biometric lock" means a device that is used to grant
20 access to a person and converts the person's biometric
21 identifier or biometric information to a mathematical
22 representation, including, but not limited to, a numeric
23 string or similar method that cannot be used to recreate the
24 person's biometric identifier.

25 "Biometric time clock" means a device that is used for
26 time management and converts a person's biometric identifier

1 or biometric information to a mathematical representation,
2 including, but not limited to, a numeric string or similar
3 method that cannot be used to recreate the person's biometric
4 identifier.

5 "Confidential and sensitive information" means personal
6 information that can be used to uniquely identify an
7 individual or an individual's account or property. Examples of
8 confidential and sensitive information include, but are not
9 limited to, a genetic marker, genetic testing information, a
10 unique identifier number to locate an account or property, an
11 account number, a PIN number, a pass code, a driver's license
12 number, or a social security number.

13 "Electronic signature" means an electronic sound, symbol,
14 or process attached to or logically associated with a record
15 and executed or adopted by a person with the intent to sign the
16 record.

17 "Person" means a natural person. A person does not include
18 an individual a private entity has no knowing contact with, or
19 awareness of.

20 "Private entity" means any individual, partnership,
21 corporation, limited liability company, association, or other
22 group, however organized. A private entity does not include a
23 State or local government agency. A private entity does not
24 include any court of Illinois, a clerk of the court, or a judge
25 or justice thereof.

26 "Security purpose" means for the purpose of preventing or

1 investigating retail theft, fraud, or any other
2 misappropriation or theft of a thing of value. "Security
3 purpose" includes protecting property from trespass,
4 controlling access to property, or protecting any person from
5 harm, including stalking, violence, or harassment, and
6 includes assisting a law enforcement investigation.

7 "Written release" means informed written consent,
8 electronic signature, or, in the context of employment, a
9 release executed by an employee as a condition of employment.

10 (Source: P.A. 103-769, eff. 8-2-24.)

11 (740 ILCS 14/15)

12 Sec. 15. Retention; collection; disclosure; destruction.

13 (a) A private entity in possession of biometric
14 identifiers or biometric information must develop a written
15 policy, made available to the person from whom biometric
16 information is to be collected or was collected ~~public~~,
17 establishing a retention schedule and guidelines for
18 permanently destroying biometric identifiers and biometric
19 information when the initial purpose for collecting or
20 obtaining such identifiers or information has been satisfied
21 or within 3 years of the individual's last interaction with
22 the private entity, whichever occurs first. Absent a valid
23 order, warrant, or subpoena issued by a court of competent
24 jurisdiction or a local or federal governmental agency, a
25 private entity in possession of biometric identifiers or

1 biometric information must comply with its established
2 retention schedule and destruction guidelines.

3 (b) No private entity may collect, capture, purchase,
4 receive through trade, or otherwise obtain a person's or a
5 customer's biometric identifier or biometric information,
6 unless it first:

7 (1) informs the subject or the subject's legally
8 authorized representative in writing that a biometric
9 identifier or biometric information is being collected or
10 stored;

11 (2) informs the subject or the subject's legally
12 authorized representative in writing of the specific
13 purpose and length of term for which a biometric
14 identifier or biometric information is being collected,
15 stored, and used; and

16 (3) receives a written release executed by the subject
17 of the biometric identifier or biometric information or
18 the subject's legally authorized representative.

19 (b-5) A private entity may collect, capture, or otherwise
20 obtain a person's or a customer's biometric identifier or
21 biometric information without satisfying the requirements of
22 subsection (b) if:

23 (1) the private entity collects, captures, or
24 otherwise obtains a person's or a customer's biometric
25 identifier or biometric information for a security
26 purpose;

1 (2) the private entity uses the biometric identifier
2 or biometric information only for a security purpose;

3 (3) the private entity retains the biometric
4 identifier or biometric information no longer than is
5 reasonably necessary to satisfy a security purpose; and

6 (4) the private entity documents a process and time
7 frame to delete any biometric information used for the
8 purposes identified in this subsection.

9 (c) No private entity in possession of a biometric
10 identifier or biometric information may sell, lease, trade, or
11 otherwise profit from a person's or a customer's biometric
12 identifier or biometric information.

13 (d) No private entity in possession of a biometric
14 identifier or biometric information may disclose, redisclose,
15 or otherwise disseminate a person's or a customer's biometric
16 identifier or biometric information unless:

17 (1) the subject of the biometric identifier or
18 biometric information or the subject's legally authorized
19 representative consents to the disclosure or redisclosure;

20 (2) the disclosure or redisclosure completes a
21 financial transaction requested or authorized by the
22 subject of the biometric identifier or the biometric
23 information or the subject's legally authorized
24 representative;

25 (3) the disclosure or redisclosure is required by
26 State or federal law or municipal ordinance; or

1 (4) the disclosure is required pursuant to a valid
2 warrant or subpoena issued by a court of competent
3 jurisdiction.

4 (e) A private entity in possession of a biometric
5 identifier or biometric information shall:

6 (1) store, transmit, and protect from disclosure all
7 biometric identifiers and biometric information using the
8 reasonable standard of care within the private entity's
9 industry; and

10 (2) store, transmit, and protect from disclosure all
11 biometric identifiers and biometric information in a
12 manner that is the same as or more protective than the
13 manner in which the private entity stores, transmits, and
14 protects other confidential and sensitive information.

15 (Source: P.A. 95-994, eff. 10-3-08.)

16 (740 ILCS 14/20)

17 Sec. 20. Right of action.

18 (a) Any person aggrieved by a violation of this Act shall
19 have a right of action in a State circuit court or as a
20 supplemental claim in federal district court against an
21 offending party, which shall be commenced within one year
22 after the cause of action accrued if, prior to initiating any
23 action against a private entity, the aggrieved person provides
24 a private entity 30 days' written notice identifying the
25 specific provisions of this Act the aggrieved person alleges

1 have been or are being violated. If, within the 30 days, the
2 private entity actually cures the noticed violation and
3 provides the aggrieved person an express written statement
4 that the violation has been cured and that no further
5 violations shall occur, no action for individual statutory
6 damages or class-wide statutory damages may be initiated
7 against the private entity. If a private entity continues to
8 violate this Act in breach of the express written statement
9 provided to the aggrieved person under this Section, the
10 aggrieved person may initiate an action against the private
11 entity to enforce the written statement and may pursue
12 statutory damages for each breach of the express written
13 statement and any other violation that postdates the written
14 statement.

15 (b) A prevailing party may recover for each violation:

16 (1) against a private entity that negligently violates
17 a provision of this Act, liquidated damages of \$1,000 or
18 actual damages, whichever is greater;

19 (2) against a private entity that intentionally or
20 recklessly violates a provision of this Act, liquidated
21 damages of \$5,000 or actual damages, whichever is greater;

22 (3) reasonable attorneys' fees and costs, including
23 expert witness fees and other litigation expenses; and

24 (4) other relief, including an injunction, as the
25 State or federal court may deem appropriate.

26 (b) For purposes of subsection (b) of Section 15, a

1 private entity that, in more than one instance, collects,
2 captures, purchases, receives through trade, or otherwise
3 obtains the same biometric identifier or biometric information
4 from the same person using the same method of collection in
5 violation of subsection (b) of Section 15 has committed a
6 single violation of subsection (b) of Section 15 for which the
7 aggrieved person is entitled to, at most, one recovery under
8 this Section.

9 (c) For purposes of subsection (d) of Section 15, a
10 private entity that, in more than one instance, discloses,
11 rediscloses, or otherwise disseminates the same biometric
12 identifier or biometric information from the same person to
13 the same recipient using the same method of collection in
14 violation of subsection (d) of Section 15 has committed a
15 single violation of subsection (d) of Section 15 for which the
16 aggrieved person is entitled to, at most, one recovery under
17 this Section regardless of the number of times the private
18 entity disclosed, redisclosed, or otherwise disseminated the
19 same biometric identifier or biometric information of the same
20 person to the same recipient.

21 (Source: P.A. 103-769, eff. 8-2-24.)

22 (740 ILCS 14/25)

23 Sec. 25. Construction.

24 (a) Nothing in this Act shall be construed to impact the
25 admission or discovery of biometric identifiers and biometric

1 information in any action of any kind in any court, or before
2 any tribunal, board, agency, or person.

3 (b) Nothing in this Act shall be construed to conflict
4 with the X-Ray Retention Act, the federal Health Insurance
5 Portability and Accountability Act of 1996, and the rules
6 promulgated under either Act.

7 (c) Nothing in this Act shall be deemed to apply in any
8 manner to a financial institution or an affiliate of a
9 financial institution that is subject to Title V of the
10 federal Gramm-Leach-Bliley Act of 1999 and the rules
11 promulgated thereunder.

12 (d) Nothing in this Act shall be construed to conflict
13 with the Private Detective, Private Alarm, Private Security,
14 Fingerprint Vendor, and Locksmith Act of 2004 and the rules
15 promulgated thereunder or information captured by an alarm
16 system as defined by that Act installed by a person licensed
17 under that Act and the rules adopted thereunder.

18 (e) Nothing in this Act shall be construed to apply to a
19 contractor, subcontractor, or agent of a State or federal
20 agency or local unit of government when working for that State
21 or federal agency or local unit of government.

22 (f) Nothing in this Act shall be construed to apply to
23 information captured by a biometric time clock or biometric
24 lock that converts a person's biometric identifier or
25 biometric information to a mathematical representation,
26 including, but not limited to, a numeric string or similar

1 method that cannot be used to recreate the person's biometric
2 identifier or biometric information.

3 (g) Nothing in this Act shall be construed to apply to a
4 private entity if the private entity's employees are covered
5 by a collective bargaining agreement that provides for
6 different policies regarding the retention, collection,
7 disclosure, and destruction of biometric information.

8 (Source: P.A. 95-994, eff. 10-3-08.)

9 Section 99. Effective date. This Act takes effect upon
10 becoming law.