



103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

HB5635

Introduced 2/9/2024, by Rep. Jeff Keicher

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 definitions of "biometric identifier" and "written release". Defines "biometric lock", "biometric time clock", "electronic signature", "person", and "security purpose". Provides that if the biometric identifier or biometric information is collected or captured for the same repeated process, the private entity is only required to inform the subject or receive consent during the initial collection. 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. Effective immediately.

LRB103 39209 JRC 69359 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 identifiers do not include information captured and converted
9 to a mathematical representation, including, but not limited
10 to, a numeric string or similar method that cannot be used to
11 recreate the biometric identifier. Biometric identifiers do
12 not include information that cannot reasonably be used to
13 identify an individual.

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

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

26 "Biometric time clock" means a device that is used for

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

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

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

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

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

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

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

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

12 (740 ILCS 14/15)

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

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

1 private entity in possession of biometric identifiers or
2 biometric information must comply with its established
3 retention schedule and destruction guidelines.

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

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

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

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

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

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

1 purpose;

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

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

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

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

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

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

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

26 (3) the disclosure or redisclosure is required by

1 State or federal law or municipal ordinance; or

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

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

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

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

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

17 (740 ILCS 14/20)

18 Sec. 20. Right of action.

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

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

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

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

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

24 (740 ILCS 14/25)

25 Sec. 25. Construction.

1 (a) Nothing in this Act shall be construed to impact the
2 admission or discovery of biometric identifiers and biometric
3 information in any action of any kind in any court, or before
4 any tribunal, board, agency, or person.

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

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

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

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

24 (f) Nothing in this Act shall be construed to apply to
25 information captured by a biometric time clock or biometric
26 lock that converts a person's biometric identifier or

1 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 or biometric information.

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

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

11 Section 99. Effective date. This Act takes effect upon
12 becoming law.