



103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

HB2252

Introduced 2/14/2023, by Rep. Dan Ugaste

SYNOPSIS AS INTRODUCED:

740 ILCS 14/5
740 ILCS 14/10
740 ILCS 14/15
740 ILCS 14/20
740 ILCS 14/25

Amends the Biometric Information Privacy Act. Changes the term "written release" to "written consent". Provides that the written policy that is developed by a private entity in possession of biometric identifiers shall be made available to the person from whom biometric information is to be collected or was collected (rather than to the public). Provides that an action brought under the Act shall be commenced within one year after the cause of action accrued if, prior to initiating any action against a private entity, the aggrieved person provides a private entity 30 days' written notice identifying the specific provisions the aggrieved person alleges have been or are being violated. Provides that if within the 30 days the private entity actually cures the noticed violation and provides the aggrieved person an express written statement that the violation has been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the private entity. Provides that if a private entity continues to violate the Act in breach of the express written statement, the aggrieved person may initiate an action against the private entity to enforce the written statement and may pursue statutory damages for each breach of the express written statement and any other violation that postdates the written statement. Provides that a prevailing party may recover: against a private entity that negligently violates the Act, actual damages (rather than liquidated damages of \$1,000 or actual damages, whichever is greater); or against a private entity that willfully (rather than intentionally or recklessly) violates the Act, actual damages plus liquidated damages up to the amount of actual damages (rather than liquidated damages of \$5,000 or actual damages, whichever is greater). Provides that the Act does not apply to a private entity if the private entity's employees are covered by a collective bargaining agreement that provides for different policies regarding the retention, collection, disclosure, and destruction of biometric information. Makes other changes.

LRB103 25586 LNS 51935 b

A BILL FOR

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 5, 10, 15, 20, and 25 as follows:

6 (740 ILCS 14/5)

7 Sec. 5. Legislative findings; intent. The General Assembly
8 finds all of the following:

9 (a) The use of biometrics is growing in the business and
10 security screening sectors and appears to promise streamlined
11 financial transactions and security screenings.

12 (b) Major national corporations have selected the City of
13 Chicago and other locations in this State as pilot testing
14 sites for new applications of biometric-facilitated financial
15 transactions, including finger-scan technologies at grocery
16 stores, gas stations, and school cafeterias.

17 (c) Biometrics are unlike other unique identifiers that
18 are used to access finances or other sensitive information.
19 For example, social security numbers, when compromised, can be
20 changed. Biometrics, however, are biologically unique to the
21 individual; therefore, once compromised, the individual has no
22 recourse, is at heightened risk for identity theft, and is
23 likely to withdraw from biometric-facilitated transactions.

1 (d) An overwhelming majority of members of the public are
2 wary ~~weary~~ of the use of biometrics when such information is
3 tied to finances and other personal information.

4 (e) Despite limited State law regulating the collection,
5 use, safeguarding, and storage of biometrics, many members of
6 the public are deterred from partaking in biometric
7 identifier-facilitated transactions.

8 (f) The full ramifications of biometric technology are not
9 fully known.

10 (g) The public welfare, security, and safety will be
11 served by regulating the collection, use, safeguarding,
12 handling, storage, retention, and destruction of biometric
13 identifiers and information.

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

15 (740 ILCS 14/10)

16 Sec. 10. Definitions. In this Act:

17 "Biometric identifier" means a retina or iris scan,
18 fingerprint, voiceprint, or scan of hand or face geometry.
19 Biometric identifiers do not include writing samples, written
20 signatures, photographs, human biological samples used for
21 valid scientific testing or screening, demographic data,
22 tattoo descriptions, or physical descriptions such as height,
23 weight, hair color, or eye color. Biometric identifiers do not
24 include donated organs, tissues, or parts as defined in the
25 Illinois Anatomical Gift Act or blood or serum stored on

1 behalf of recipients or potential recipients of living or
2 cadaveric transplants and obtained or stored by a federally
3 designated organ procurement agency. Biometric identifiers do
4 not include biological materials regulated under the Genetic
5 Information Privacy Act. Biometric identifiers do not include
6 information captured from a patient in a health care setting
7 or information collected, used, or stored for health care
8 treatment, payment, or operations under the federal Health
9 Insurance Portability and Accountability Act of 1996.
10 Biometric identifiers do not include an X-ray, roentgen
11 process, computed tomography, MRI, PET scan, mammography, or
12 other image or film of the human anatomy used to diagnose,
13 prognose, or treat an illness or other medical condition or to
14 further validate scientific testing or screening.

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

23 "Confidential and sensitive information" means personal
24 information that can be used to uniquely identify an
25 individual or an individual's account or property. Examples of
26 confidential and sensitive information include, but are not

1 limited to, a genetic marker, genetic testing information, a
2 unique identifier number to locate an account or property, an
3 account number, a PIN number, a pass code, a driver's license
4 number, or a social security number.

5 "Private entity" means any individual, partnership,
6 corporation, limited liability company, association, or other
7 group, however organized. A private entity does not include a
8 State or local government agency. A private entity does not
9 include any court of Illinois, a clerk of the court, or a judge
10 or justice thereof.

11 "Written consent ~~release~~" means informed written consent
12 ~~or, in the context of employment, a release executed by an~~
13 ~~employee as a condition of employment.~~

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

15 (740 ILCS 14/15)

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

17 (a) A private entity in possession of biometric
18 identifiers or biometric information must develop a written
19 policy, made available to the person from whom biometric
20 information is to be collected or was collected ~~public~~,
21 establishing a retention schedule and guidelines for
22 permanently destroying biometric identifiers and biometric
23 information when the initial purpose for collecting or
24 obtaining such identifiers or information has been satisfied
25 or within 3 years of the individual's last interaction with

1 the private entity, whichever occurs first. Absent a valid
2 order, warrant, or subpoena issued by a court of competent
3 jurisdiction or a local or federal governmental agency, a
4 private entity in possession of biometric identifiers or
5 biometric information must comply with its established
6 retention schedule and destruction guidelines.

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

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

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

20 (3) receives a written consent ~~release~~ executed by the
21 subject of the biometric identifier or biometric
22 information or the subject's legally authorized
23 representative.

24 Written consent may be obtained by electronic means.

25 (c) No private entity in possession of a biometric
26 identifier or biometric information may sell, lease, trade, or

1 otherwise profit from a person's or a customer's biometric
2 identifier or biometric information.

3 (d) No private entity in possession of a biometric
4 identifier or biometric information may disclose, redisclose,
5 or otherwise disseminate a person's or a customer's biometric
6 identifier or biometric information unless:

7 (1) the subject of the biometric identifier or
8 biometric information or the subject's legally authorized
9 representative provides written consent ~~consents~~ to the
10 disclosure or redisclosure;

11 (2) the disclosure or redisclosure completes a
12 financial transaction requested or authorized by the
13 subject of the biometric identifier or the biometric
14 information or the subject's legally authorized
15 representative;

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

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

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

23 (1) store, transmit, and protect from disclosure all
24 biometric identifiers and biometric information using the
25 reasonable standard of care within the private entity's
26 industry; and

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

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

7 (740 ILCS 14/20)

8 Sec. 20. Right of action. Any person aggrieved by a
9 violation of this Act shall have a right of action in a State
10 circuit court or as a supplemental claim in federal district
11 court against an offending party, which shall be commenced
12 within one year after the cause of action accrued if, prior to
13 initiating any action against a private entity, the aggrieved
14 person provides a private entity 30 days' written notice
15 identifying the specific provisions of this Act the aggrieved
16 person alleges have been or are being violated. If, within the
17 30 days, the private entity actually cures the noticed
18 violation and provides the aggrieved person an express written
19 statement that the violation has been cured and that no
20 further violations shall occur, no action for individual
21 statutory damages or class-wide statutory damages may be
22 initiated against the private entity. If a private entity
23 continues to violate this Act in breach of the express written
24 statement provided to the aggrieved person under this Section,
25 the aggrieved person may initiate an action against the

1 private entity to enforce the written statement and may pursue
2 statutory damages for each breach of the express written
3 statement and any other violation that postdates the written
4 statement. A prevailing party in any such action may recover
5 ~~for each violation:~~

6 (1) against a private entity that negligently violates
7 a provision of this Act, ~~liquidated damages of \$1,000 or~~
8 ~~actual damages, whichever is greater;~~

9 (2) against a private entity that willfully
10 ~~intentionally or recklessly~~ violates a provision of this
11 Act, actual damages plus liquidated damages up to the
12 amount of actual damages ~~of \$5,000 or actual damages,~~
13 ~~whichever is greater;~~

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

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

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

19 (740 ILCS 14/25)

20 Sec. 25. Construction.

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

25 (b) Nothing in this Act shall be construed to conflict

1 with the X-Ray Retention Act, the federal Health Insurance
2 Portability and Accountability Act of 1996 and the rules
3 promulgated under either Act.

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

9 (d) Nothing in this Act shall be construed to conflict
10 with the Private Detective, Private Alarm, Private Security,
11 Fingerprint Vendor, and Locksmith Act of 2004 and the rules
12 promulgated thereunder.

13 (e) Nothing in this Act shall be construed to apply to a
14 contractor, subcontractor, or agent of a State or federal
15 agency or local unit of government when working for that State
16 or federal agency or local unit of government.

17 (f) Nothing in this Act shall be construed to apply to a
18 private entity if the private entity's employees are covered
19 by a collective bargaining agreement that provides for
20 different policies regarding the retention, collection,
21 disclosure, and destruction of biometric information.

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