SB3856

LRB104 17142 JRC 30561 b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

SB3856

Introduced 2/6/2026, by Sen. John F. Curran

SYNOPSIS AS INTRODUCED:

740 ILCS 14/10
740 ILCS 14/15

Amends the Biometric Information Privacy Act. Defines "security purpose" to mean for the purpose of preventing or investigating retail theft, fraud, or any other misappropriation or theft of a thing of value. Provides that security purpose includes protecting property from trespass, controlling access to property, or protecting any person from harm, including stalking, violence, or harassment, and includes assisting a law enforcement investigation. 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. Effective immediately.

LRB104 17142 JRC 30561 b

A BILL FOR

AN ACT concerning civil law.

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

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

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

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

treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

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

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

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

"Private entity" means any individual, partnership,

corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

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

"Written release" means informed written consent, electronic signature, or, in the context of employment, a release executed by an employee as a condition of employment. (Source: P.A. 103-769, eff. 8-2-24.)

(740 ILCS 14/15)

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

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last

interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

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

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

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

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

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

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

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

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

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

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

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

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

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric

information or the subject's legally authorized representative;

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

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

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

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

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

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

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