

AN ACT concerning health.

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

Section 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

Section 5. Legislative findings; intent. The General Assembly finds all of the following:

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

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

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

(d) An overwhelming majority of members of the public are

weary of the use of biometrics when such information is tied to finances and other personal information.

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

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

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

Section 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.

"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.

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

Section 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.

(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.

Section 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

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

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

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

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

Section 25. Construction.

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

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

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

(d) Nothing in this Act shall be construed to conflict with

the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

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

Section 30. Biometric Information Privacy Study Committee.

(a) The Department of Human Services, in conjunction with Central Management Services, subject to appropriation or other funds made available for this purpose, shall create the Biometric Information Privacy Study Committee, hereafter referred to as the Committee. The Department of Human Services, in conjunction with Central Management Services, shall provide staff and administrative support to the Committee. The Committee shall examine (i) current policies, procedures, and practices used by State and local governments to protect an individual against unauthorized disclosure of his or her biometric identifiers and biometric information when State or local government requires the individual to provide his or her biometric identifiers to an officer or agency of the State or local government; (ii) issues related to the collection, destruction, security, and ramifications of biometric identifiers, biometric information, and biometric technology; and (iii) technical and procedural changes necessary in order

to implement and enforce reasonable, uniform biometric safeguards by State and local government agencies.

(b) The Committee shall hold such public hearings as it deems necessary and present a report of its findings and recommendations to the General Assembly before January 1, 2009. The Committee may begin to conduct business upon appointment of a majority of its members. All appointments shall be completed by 4 months prior to the release of the Committee's final report. The Committee shall meet at least twice and at other times at the call of the chair and may conduct meetings by telecommunication, where possible, in order to minimize travel expenses. The Committee shall consist of 27 members appointed as follows:

- (1) 2 members appointed by the President of the Senate;
- (2) 2 members appointed by the Minority Leader of the Senate;
- (3) 2 members appointed by the Speaker of the House of Representatives;
- (4) 2 members appointed by the Minority Leader of the House of Representatives;
- (5) One member representing the Office of the Governor, appointed by the Governor;
- (6) One member, who shall serve as the chairperson of the Committee, representing the Office of the Attorney General, appointed by the Attorney General;
- (7) One member representing the Office of the Secretary

of the State, appointed by the Secretary of State;

(8) One member from each of the following State agencies appointed by their respective heads: Department of Corrections, Department of Public Health, Department of Human Services, Central Management Services, Illinois Commerce Commission, Illinois State Police, Department of Revenue;

(9) One member appointed by the chairperson of the Committee, representing the interests of the City of Chicago;

(10) 2 members appointed by the chairperson of the Committee, representing the interests of other municipalities;

(11) 2 members appointed by the chairperson of the Committee, representing the interests of public hospitals; and

(12) 4 public members appointed by the chairperson of the Committee, representing the interests of the civil liberties community, the electronic privacy community, and government employees.

(c) This Section is repealed January 1, 2009.

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