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 "Pay By Touch" at banks, 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

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

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

(f) 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 any indelible personal physical characteristic which can be used to uniquely identify an individual or pinpoint an individual at a particular place at a particular time. Examples of biometric identifiers include, but are not limited to iris or retinal scans, fingerprints, voiceprints, and records or scans of hand geometry, facial geometry, or facial recognition. Biometric identifiers do not include writing samples, written signatures, photographs, tattoo descriptions, physical descriptions, or human biological samples used for valid scientific testing or screening. 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 valid 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. Biometric information does 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.

"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.

"Legally effective written release" means informed written consent or a release executed by an employee as a condition of employment.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a public agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Public agency" means the State of Illinois and its various subdivisions and agencies, and all units of local government, school districts, and other governmental entities. A public agency does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

Section 15. Retention; collection; disclosure; destruction.

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

(b) No public agency or 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 in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject 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 legally effective written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) Subsections (a) and (b) of this Section do not apply to a public agency:

(1) engaged in criminal investigations, arrests,

prosecutions, or law enforcement;

(2) overseeing pretrial detention, post-trial commitment, corrections or incarceration, civil commitment, probation services, or parole services;

(3) serving as the State central repository of biometrics for criminal identification and investigation purposes;

(4) furnishing biometric identifiers or biometric information to a State or federal repository of biometrics pursuant to State or federal law or municipal ordinance;

(5) receiving biometric identifiers or biometric information pursuant to State or federal law or municipal ordinance;

(6) acting pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction;

(7) issuing driver's licenses, driver's permits, identification cards issued pursuant to the Illinois Identification Card Act, or occupational licenses; or

(8) performing employee background checks in accordance with the public agency's hiring policies or statutory obligations.

Nothing in subsections (a) and (b) of this Section shall be construed to conflict with the retention and collection practices for fingerprints, other biometric identifiers, or biometric information under the Criminal Identification Act, the Illinois Uniform Conviction Information Act, or the federal

National Crime Prevention and Privacy Compact. Subsection (a) of this Section does not apply to school districts; however, a school district that collects biometric identifiers or biometric information must adopt retention schedules and destruction policies in accordance with the School Code. Subsection (a) of this Section does not apply to a fingerprint vendor or fingerprint vendor agency; however, a fingerprint vendor or fingerprint vendor agency must adopt retention schedules and destruction policies in accordance with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004.

(d) No public agency or 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.

(e) No public agency or 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;

(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.

(f) Nothing in subsections (d) or (e) of this Section shall be construed to prohibit or inhibit a public agency (i) engaged in criminal investigations, arrests, prosecutions, or law enforcement, (ii) overseeing pretrial detention, post-trial commitment, corrections or incarceration, civil commitment, probation services, or parole services, (iii) serving as the State central repository of biometrics for criminal identification and investigation purposes, (iv) furnishing biometric identifiers or biometric information to a State or federal repository of biometrics pursuant to State or federal law, or (v) issuing driver's licenses, driver's permits, or identification cards pursuant to the Illinois Identification Card Act from:

(1) sharing biometric identifiers or biometric information with another public agency engaged in criminal investigations, arrests, prosecutions, or law enforcement to further such criminal investigations, arrests, prosecutions, or law enforcement;

(2) sharing biometric identifiers or biometric information with another public agency overseeing pretrial detention, post-trial commitment, corrections or

incarceration, civil commitment, probation services, or parole services;

(3) sharing biometric identifiers or biometric information pursuant to, or required by, State or federal law; or

(4) sharing biometric identifiers or biometric information pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(g) Nothing in subsections (d) or (e) of this Section shall be construed to conflict with the reporting and sharing practices for fingerprints, other biometric identifiers, or biometric information under the Criminal Identification Act, the Illinois Uniform Conviction Information Act, and the federal National Crime Prevention and Privacy Compact. Nothing in subsection (d) of this Section shall be construed to conflict with the reporting and sharing practices of a fingerprint vendor or fingerprint vendor agency under the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004.

(h) Nothing in subsections (d) or (e) of this Section shall be construed to prohibit or inhibit a public agency that issues occupational licenses from:

(1) sharing biometric identifiers or biometric information pursuant to or when required by State or federal law; or

(2) sharing biometric identifiers or biometric

information pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(i) Nothing in subsections (d) or (e) of this Section shall be construed to prohibit a public agency from performing employee background checks in accordance with the public agency's hiring policies or statutory obligations.

(j) A public agency in possession of biometric identifiers or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information in a reasonable manner that is the same as or more protective than the manner in which the public agency stores, transmits, and protects other similar confidential and sensitive information specific to that public agency. The storage, transmittal, and protection from disclosure standards under this subsection (j) are solely the choice of the public agency to adopt in accordance with this Act, other applicable State or federal law, evolving advances in technology, budget constraints, and comparable practices specific to that public agency.

(k) 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.

(l) All information and records held by a public agency pertaining to biometric identifiers and biometric information shall be confidential and exempt from copying and inspection under the Freedom of Information Act to all except to the subject of the biometric identifier or biometric information. The subject of the biometric identifier or biometric information held by a public agency shall be permitted to copy and inspect only their own biometric identifiers and biometric 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 any public agency or private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against any public agency or 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. 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. Nothing in this Act shall be construed to conflict with the X-Ray Retention Act or the federal Health Insurance Portability and Accountability Act of 1996. Subcontractors or agents of a public agency must comply with this Act to the extent and manner this Act applies to that public agency.

Section 30. Home rule. Any home rule unit of local government, any non-home rule municipality, or any non-home rule county within the unincorporated territory of the county may enact ordinances, standards, rules, or regulations that protect biometric identifiers and biometric information in a manner or to an extent equal to or greater than the protection provided in this Act. This Section is a limitation on the concurrent exercise of home rule power under subsection (i) of Section 6 of Article VII of the Illinois Constitution.

Section 95. Applicability. This Act applies to private

entities beginning on the effective date of this Act. This Act applies to public agencies beginning on January 1, 2011.

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