By: Representatives Porter, Anthony, Hulum, Foster

To: Judiciary A

HOUSE BILL NO. 467

AN ACT TO CREATE THE "BIOMETRIC IDENTIFIERS PRIVACY ACT"; TO PROVIDE LEGISLATIVE FINDINGS; TO DEFINE TERMS RELATING TO BIOMETRIC IDENTIFIERS; TO REQUIRE PRIVATE ENTITIES IN POSSESSION OF BIOMETRIC IDENTIFIERS TO DEVELOP A POLICY THAT ESTABLISHES A RETENTION SCHEDULE AND GUIDELINES FOR DESTROYING THE BIOMETRIC IDENTIFIERS OF INDIVIDUALS; TO PROVIDE CERTAIN REQUIREMENTS AND RESTRICTIONS FOR PRIVATE ENTITIES THAT COLLECT BIOMETRIC IDENTIFIERS; TO PROVIDE THAT UPON THE REQUEST OF AN INDIVIDUAL, A PRIVATE ENTITY THAT COLLECTS BIOMETRIC IDENTIFIERS SHALL DISCLOSE TO THE INDIVIDUAL HIS OR HER BIOMETRIC IDENTIFIER AND INFORMATION RELATED TO THE USE OF SUCH BIOMETRIC IDENTIFIER; TO PROVIDE FOR A RIGHT OF ACTION FOR INDIVIDUALS ALLEGING A VIOLATION OF THIS ACT; TO PROVIDE THAT THE ATTORNEY GENERAL MAY BRING AN ACTION AGAINST A PRIVATE ENTITY WHO VIOLATES THE PROVISIONS OF THIS ACT; AND FOR RELATED PURPOSES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MISSISSIPPI:

SECTION 1. This act shall be known and may be cited as the "Biometric Identifiers Privacy Act".

SECTION 2. The Legislature finds the following:

(a) Businesses are increasingly using biometrics to attempt to verify customer identity, streamline transactions, control access to secure areas and maximize revenues.

(b) Biometrics are unlike other unique identifiers that are used to verify identity or 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.

(c) The public has grown wary of the use of biometrics because of concerns about the security of protecting such information once it is captured and stored without their consent. Indeed, recent data breaches have exposed people's biometric identifiers, leaving people vulnerable to harm.

(d) Additionally, biometric identifiers can be collected without people's knowledge, applied instantaneously to identify people in circumstances where they have an expectation of privacy and anonymity, and used to identify and track people's movements, activities and associations.

(e) Studies have also shown that one increasingly prevalent biometric collection and matching technology, facial recognition technology, has worse misidentification and misclassification rates when used on the faces of people of color, women, children, persons who are elderly, and transgender and non-binary persons. This has led to documented cases of businesses refusing admission or service to people because facial recognition systems incorrectly "matched" them to photos of suspected shoplifters or others who had been barred from the premises.

(f) The lack of legal protections regulating the collection, use, safeguarding and storage of biometrics means that many members of the public fear that their biometric identifiers may be collected and used without their knowledge and consent.

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

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

SECTION 3. As used in this act, the following words shall have the meanings as defined in this section, unless the context clearly requires otherwise:

(a) "Biometric identifier" means the data of an individual generated by measurements of an individual's unique biological characteristics such as a faceprint, fingerprint, voiceprint, retina or iris image, or any other biological characteristic that can be used to uniquely identify the individual. "Biometric identifier" does not include:

(i) A writing sample of written signature;

(ii) A photograph or video, except "biometric identifier" includes data generated, captured, or collected from the biological characteristics of a person depicted in a photograph or video;

(iii) A human biological sample used for valid scientific testing or screening;

(iv) Demographic data;

(v) A physical description, including height, weight, hair color, eye color, or a tattoo description;

(vi) Any donated portion of a human body stored on behalf of a recipient of potential recipient of a living cadaveric transplant and obtained or stored by a federally designated organ procurement agency, including an organ, tissue, eye, bone, artery, blood, and any other fluid or serum;

(vii) Information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountably Act of 1996;

(viii) Any image or film of the human anatomy used to diagnose, provide a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening including an x-ray, roentgen process, computed tomography, magnetic resonance imaging image, positron emission tomography scan, and mammography; or

(ix) Information collected, used, or disclosed for human subject research that is conducted in accordance with the federal policy for the protection of human subjects, under 45 C.F.R. Part 46, or other similar research ethics laws, or with the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

(b) "Private entity" means any individual acting in a commercial context, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a state or local government agency or entity.

(c) "Verified request" means a request that is made by a person or by an individual authorized to act as that person's representative, and that the private entity can verify, using commercially reasonable methods, to be the person whose biometric identifiers the private entity collected.

(d) "Written release" means informed written consent, including written consent provided by electronic means. A valid written release may not be secured through a general release or user agreement.

(i) In the context of employment, a written release:

1. May only be used to secure consent to collect and use biometric identifiers for the purposes of:

(A) Permitting access to secure physical locations and secure electronic hardware and software applications, without retaining data that allows for employee location tracking or the tracking of how long an employee spends using a hardware or software application; or

(B) Recording the commencement and conclusion of an employee's full work day and meal/rest breaks in excess of 30 minutes;

2. May be secured in the form of a written release executed by an employee as a condition of employment.

SECTION 4. (1) A private entity in possession of biometric identifiers must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying a biometric identifier of an individual on the earliest of:

(a) The date on which the initial purpose for collecting or obtaining the biometric identifier has been satisfied;

(b) One (1) year after the individual's last interaction with the private entity; or

(c) Thirty (30) days after receiving a verified request to delete the biometric identifiers submitted by the individual or the individual's representative.

(2) Absent a valid warrant or subpoena issued by a court of competent jurisdiction, or a compulsory request or demand issued by a state agency in an investigation of a violation of this act, a private entity in possession of biometric identifiers must comply with its established retention schedule and destruction guidelines.

(3) A private entity is not required to make available to the public a written policy that:

(a) Applies only to employees of that private entity; and

(b) Is used solely within the private entity for operation of the private entity.

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

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

(b) 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 is being collected, stored and used; and

(c) Receives a written release executed by the subject of the biometric identifier or the subject's legally authorized representative.

(5) No private entity that collects a person's biometric identifier shall:

(a) Sell, lease, or trade such biometric identifier; or

(b) Permit any entity to which a biometric identifier is transferred, shared, or provided to sell, lease, or trade such biometric identifier.

(6) No private entity that collects a biometric identifier shall disclose, redisclose, or otherwise disseminate a person's biometric identifier unless:

(a) The subject of the biometric identifier or the subject's legally authorized representative executes a written release consenting to the specific disclosure or redisclosure;

(b) The disclosure or redisciosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the subject's legally authorized representative;

(c) The disclosure or redisclosure is required by state or federal law or municipal ordinance; or

(d) The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction, or a compulsory request or demand issued by a state agency in an investigation of a violation of this act.

(7) A private entity shall not:

(a) Condition the provision of a good or service on the collection, use, disclosure, transfer, sale, retention, or processing of biometric identifiers, unless biometric identifiers are strictly necessary to provide the good or service; or

(b) Charge different prices or rates for goods or services or provide a different level of quality of a good or service to any individual who exercises the individual's rights under this act.

(8) A private entity in possession of a biometric identifier shall:

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

(b) Store, transmit, and protect from disclosure all biometric identifiers 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 5. (1) At the request of an individual or an individual's legally authorized representative, a private entity that collects biometric identifiers shall disclose to the individual, free of charge, the individual's biometric identifier and information related to the use of the biometric identifier, including:

(a) The precise type of biometric identifiers that were collected and/or used;

(b) The specific sources from which the private entity collected the biometric identifiers;

(c) The specific purpose for which the private entity used the biometric identifiers and personal information;

(d) The identities of third parties with whom the private entity shares the biometric identifiers and the purposes of sharing; and

(e) The specific biometric identifiers that the business discloses to third parties.

(2) The requirements of this section shall only apply to:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that: (i) does business in the State of Mississippi, (ii) is organized or operated for the financial benefit of its shareholders or other owners, (iii) collects consumers' biometric identifiers or has such identifiers collected on its behalf, and (iv) had annual gross revenues in excess of Ten Million Dollars ($10,000,000.00), in the preceding calendar year.

(b) Any entity that controls or is controlled by a business as described in paragraph (2)(a) of this Section 5, and that shares common branding with the business and with whom the business shares consumers' personal information. As used in this act, the word "control" and "controlled" means ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. As used in this act, the word "common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(c) A joint venture or partnership composed of businesses in which each business has at least a forty percent (40%) interest. The joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

SECTION 6. (1) An individual alleging a violation of this act may bring a civil action against the offending private entity in a court of competent jurisdiction. A prevailing plaintiff may recover for each violation:

(a) Against a private entity that negligently violates a provision of this act, liquidated damages of One Thousand Dollars ($1,000.00), or actual damages, whichever is greater;

(b) Against a private entity that intentionally or recklessly violates a provision of this act, liquidated damages of Five Thousand Dollars ($5,000.00), or actual damages, whichever is greater;

(c) Reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(d) Other relief, including an injunction or declaration, as the court may deem appropriate.

(2) The Attorney General may bring an action against a private entity who violates any provisions of this act, and shall be entitled to seek any forms of relief and remedies available to

private plaintiffs, including the collection of damages as a civil penalty.

SECTION 7. (1) Nothing in this act shall be construed to impact the admission or discovery of biometric identifiers in any action of any kind in any court, or before any tribunal, board, or agency.

(2) Nothing in this act shall be construed to conflict with the federal Health Insurance Portability and Accountability Act of 1996, and the rules promulgated under that act.

(3) Nothing in this act shall be deemed to apply in any manner to information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act of 1999, and the rules promulgated thereunder.

(4) 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, and such exemption shall only apply to the extent the collection, retention, and use of the biometric identifier is in direct service of the purpose for which the state agency or local unit of government retained the services of the contractor, subcontractor, or agent.

SECTION 8. If any section, paragraph, sentence, phrase or any part of this act shall be held invalid or unconstitutional, such holding shall not affect any other section, paragraph,

sentence, clause, phrase or part of this act which is not in and of itself invalid or unconstitutional.

Moreover, if the application of this act, or of any portion of it, to any person or circumstance is held invalid, the invalidity shall not affect the application of this act to other persons or circumstances which can be given effect without the invalid provision or application.

SECTION 9. This act shall take effect and be in force from and after July 1, 2023.