**A** **BILL**

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, BY ADDING CHAPTER 31 TO TITLE 37 SO AS TO ENACT THE “SOUTH CAROLINA BIOMETRIC DATA PRIVACY ACT” AND TO PROVIDE CERTAIN REQUIREMENTS FOR A BUSINESS THAT COLLECTS A CONSUMER’S BIOMETRIC INFORMATION, TO ALLOW THE CONSUMER TO REQUEST THAT A BUSINESS DELETE THE COLLECTED BIOMETRIC INFORMATION AND TO PROHIBIT THE SALE OF BIOMETRIC INFORMATION, TO ESTABLISH CERTAIN STANDARDS OF CARE FOR A BUSINESS THAT COLLECTS BIOMETRIC INFORMATION, TO ESTABLISH A PROCEDURE FOR A CONSUMER TO OPT OUT OF THE SALE OF BIOMETRIC INFORMATION, TO PROHIBIT A BUSINESS FROM DISCRIMINATING AGAINST A CONSUMER WHO OPTS OUT OF THE SALE OF THEIR BIOMETRIC INFORMATION, AND TO PROVIDE A PENALTY.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. Title 37 of the 1976 Code is amended by adding:

“CHAPTER 31

South Carolina Biometric Data Privacy Act

Section 37‑31‑10. This chapter may be known and cited as the ‘South Carolina Biometric Data Privacy Act’.

Section 37‑31‑20. For purposes of this chapter:

(1) ‘Biometric information’ means an individual’s physiological, biological, or behavioral characteristics, including the individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish an individual’s identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted and keystroke patterns of rhythms, gait patterns or rhythms, and sleep, health, exercise data, or geolocation data that contain identifying information.

(2) ‘Business’s means a corporation, general partnership, limited partnership, joint venture, trust, proprietorship, or other similar entity or organization authorized to conduct business in and operating within this State.

(3) ‘Personal information’ means information that identifies or describes an individual including, but not limited to, an individual’s photograph or digitized image, social security number, date of birth, driver’s identification number, name, home address, home telephone number, medical or disability information, education level, financial status, bank account numbers, account or identification number issued by or used, or both, by any federal or state governmental agency or private financial institution, employment history, height, weight, race, other physical details, signature, biometric identifiers, and any credit records or reports.

Section 37‑31‑30. (A) A business that collects a consumer’s biometric information shall, at or before the point of collection, inform the consumer of the specific and legitimate purpose for which the biometric information will be used and the consumer must give the business consent before any biometric information may be collected. A business may not collect any form of biometric information or use the information collected for an additional purpose without written consent of the consumer.

(B) A consumer has the right to request that a business that collects a consumer’s biometric information disclose the categories and specific pieces of information the business has collected. The business must deliver the information by mail or an easily accessible electronic method. A business may not be required to provide this information more than twice in a twelve month period.

Section 37‑31‑40. (A) A consumer may request that a business delete biometric information collected by the business once the initial purpose of the collection of biometric information has been satisfied.

(B) A business that receives a request to delete information shall delete the consumer’s biometric information from its records and direct all third party providers with records of a consumer’s biometric information to delete the information from their records.

(C) A business that receives a request to delete information shall complete this request in a timely manner. The request must be completed within one year of the date the request is received unless the information is being used to comply with law enforcement, a court order, or used to complete a financial transaction requested by the consumer.

Section 37‑31‑50. (A) A consumer has the right, at any time, to direct a business that sells biometric information about the consumer to third parties to discontinue selling the information or prohibit the sale of information. A business that has received direction to discontinue or prohibit the sale of biometric information is prohibited from selling the information after its receipt of the consumer’s direction and, if it does so, is subject to the penalties provided in this chapter.

(B) A business may not sell the biometric information of a consumer if the business has actual knowledge that the consumer is less than sixteen years of age unless the consumer’s parent or guardian has affirmatively authorized the sale of the biometric data. A business that wilfully disregards the consumer’s age is deemed to have actual knowledge of the consumer’s age.

Section 37‑31‑60. A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information:

(1) using the reasonable standard of care within the private entity’s industry; and

(2) 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 37‑31‑70. (A) A business that collects a consumer’s biometric information must:

(1) provide a clear and conspicuous link on the business’s website titled ‘Do Not Sell My Biometric Information’ to a webpage that enables a consumer or a person authorized by the consumer to opt‑out of the sale of the consumer’s biometric information. The business may not require a consumer to create an account in order to direct the business not to sell the consumer’s biometric information;

(2) include a description of a consumer’s rights pursuant to this chapter on the link provided for in item (1);

(3) ensure that all individuals responsible for handling consumer inquiries about the business’s privacy practices or the business’s compliance with the provisions of this chapter and how to direct consumers to exercise their rights;

(4) refrain from selling the biometric information collected by the business for a consumer who exercises his right to opt‑out of the sale of his biometric information;

(5) respect the consumer’s decision to opt‑out for at least one year before requesting that the consumer authorize the sale of the consumer’s biometric information; and

(6) use any of the personal information, including biometric information, collected from the consumer in connection with the submission of the consumer’s opt‑out request solely for the purposes of complying with the opt‑out request.

(B) A consumer may authorize another person to opt‑out of the sale of the consumer’s biometric information on the consumer’s behalf and the business must act in a manner consistent with an opt‑out directly from the consumer.

(C) A business may maintain a separate and additional website dedicated to South Carolina consumers that includes the required links and text. The business must take reasonable steps to ensure that South Carolina consumers are directed to the website for South Carolina consumers in lieu of a website available to the general public.

Section 37‑31‑80. (A) A business may not discriminate against a consumer who exercises any of the rights provided pursuant to the provisions of this chapter by undertaking certain actions including, but not limited to:

(1) denying goods or services to the consumer;

(2) charging different prices or rates for goods or services, including through the use of discounts, benefits, or imposing a penalty;

(3) providing a different level or quality of goods or services to the consumer; or

(4) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(B)(1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of biometric information, sale of biometric information, or the deletion of biometric information. The business may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(2) If the business elects to offer financial incentives, it must notify consumers of the financial incentive in the manner provided for in Section 37‑31‑70.

(3) The business may not offer or enter into a financial incentive program unless the consumer gives the business prior opt‑in consent which clearly describes the material terms of the incentive program pursuant to Section 37‑31‑70.

(C) Nothing in this section prohibits a business from charging a consumer a different price or rate or from providing a different level or quality of goods or services to the consumer if that difference is reasonably related to the value provided to the consumer by the consumer’s biometric information.

Section 37‑31‑90. A business that collects a consumer’s biometric information must notify all consumers of a breach of security of business data within seventy two hours of the business discovering the breach. A business that fails to notify consumers is subject to a fine of five thousand dollars for each consumer that was not notified. This fine is in addition to other penalties provided by law.

Section 37‑31‑100. (A) A person aggrieved by a violation of this chapter may bring an action against the business and any other officials acting in their official capacities who are responsible for the violation and seek appropriate relief including:

(1) against a business that negligently violates a provision of this chapter, damages of one thousand dollars or actual damages, whichever is greater;

(2) against a business that intentionally or recklessly violates a provision of this chapter, damages of ten thousand dollars or actual damages, whichever is greater;

(3) reasonable attorney’s fees and costs, including expert witness fees and other litigation expenses; and

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

(B) The provisions of this section may not be construed to limit the penalties for a breach of security of business data provided for in Section 39‑1‑90.”

SECTION 2. This act takes effect upon approval by the Governor.

‑‑‑‑XX‑‑‑‑