SENATE BILL 201

I3 0lr0986
CF 0lr0985

By: **Senator Lee**
Introduced and read first time: January 16, 2020
Assigned to: Finance

A BILL ENTITLED

AN ACT concerning

Commercial Law – Personal Information Protection Act – Revisions

FOR the purpose of requiring a business that maintains personal information of an individual residing in the State to implement and maintain certain security procedures and practices; altering the circumstances under which the owner or licensee of certain computerized data is required to notify certain individuals of a certain breach; altering the time periods within which certain notifications regarding the breach of a security system are required to be given; requiring, rather than authorizing, a certain notification to be given in a certain manner under certain circumstances; repealing a certain provision of law authorizing a certain notification to be given in a certain manner under certain circumstances; requiring certain supplemental notifications to be provided in a certain manner; requiring the notice of a certain breach provided to the Office of the Attorney General to include certain information; defining a certain term and altering the definition of a certain term; and generally relating to personal information protection.

BY repealing and reenacting, with amendments,
Article – Commercial Law
Section 14–3501, 14–3503(a), and 14–3504
Annotated Code of Maryland
(2013 Replacement Volume and 2019 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Commercial Law

14–3501.

(a) In this subtitle the following words have the meanings indicated.

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

(b) (1) "Business" means a sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit.

(2) "Business" includes a financial institution organized, chartered, licensed, or otherwise authorized under the laws of this State, any other state, the United States, or any other country, and the parent or subsidiary of a financial institution.

(c) "Encrypted" means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.

(D) "GENETIC TEST" MEANS AN ANALYSIS OF HUMAN DNA, RNA, CHROMOSOMES, PROTEINS, OR METABOLITES.

[(d)**] (E)** "Health information" means any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment or diagnosis.

[(e)**] (F)** (1) "Personal information" means:

(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government;

2. A driver's license number or State identification card number;

3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;

4. Health information, including information about an individual's mental health;

5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self–insured, that permits access to an individual's health information; **[**or**]**

6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print,

genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or

7. ACTIVITY–TRACKING DATA, INCLUDING:

A. ALL DATA COLLECTED THROUGH AN APPLICATION OR ELECTRONIC DEVICE CAPABLE OF TRACKING INDIVIDUAL ACTIVITY, BEHAVIOR, OR LOCATION; AND

B. ANY INFORMATION OR DATA DERIVED FROM DATA COLLECTED UNDER ITEM A OF THIS ITEM;

(ii) A user name or e–mail address in combination with a password or security question and answer that permits access to an individual's e–mail account**;**

(III) GENETIC INFORMATION WITH RESPECT TO AN INDIVIDUAL, INCLUDING:

1. THE GENETIC SAMPLE OF AN INDIVIDUAL;

2. A GENETIC TEST OF AN INDIVIDUAL;

3. A GENETIC TEST OF A FAMILY MEMBER OF AN INDIVIDUAL;

4. THE MANIFESTATION OF A DISEASE OR DISORDER IN A FAMILY MEMBER OF AN INDIVIDUAL;

5. ANY REQUEST FOR, OR RECEIPT OF, A GENETIC TEST, GENETIC COUNSELING, OR GENETIC EDUCATION; AND

6. ANY INFORMATION DERIVED FROM GENETIC INFORMATION WITH RESPECT TO AN INDIVIDUAL; OR

(IV) NONPUBLIC SOCIAL MEDIA INFORMATION ABOUT AN INDIVIDUAL, INCLUDING COMMUNICATIONS, POSTINGS, PICTURES, VIDEOS, CONNECTIONS BETWEEN INDIVIDUALS, CONNECTIONS BETWEEN ACCOUNTS, AND ACTIONS.

(2) "Personal information" does not include:

(i) Publicly available information that is lawfully made available to the general public from federal, State, or local government records;

(ii) Information that an individual has consented to have publicly disseminated or listed; or

(iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.

[(f)**] (G)** "Records" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

14–3503.

(a) To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns**, MAINTAINS,** or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned**, MAINTAINED,** or licensed and the nature and size of the business and its operations.

14–3504.

(a) In this section:

(1) "Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business; and

(2) "Breach of the security of a system" does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (1) A business that owns, licenses, or maintains computerized data that includes personal information of an individual residing in the State, when it discovers or is notified that it incurred a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.

(2) Subject to subsection (c)(4) of this section, **[**if, after the investigation is concluded,**]** **UNLESS** the business **REASONABLY** determines that the breach of the security of the system **[**creates**]** **DOES NOT CREATE** a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach.

(3) Except as provided in subsection (d) of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably

practicable, but not later than **[**45**]** **30** days after the business **[**concludes the investigation required under paragraph (1) of this subsection**]** **DISCOVERS OR IS NOTIFIED OF THE BREACH OF THE SECURITY OF A SYSTEM**.

(4) If after the investigation required under paragraph (1) of this subsection is concluded, the business determines that notification under paragraph (2) of this subsection is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made.

(c) (1) A business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license, when it discovers or is notified of a breach of the security of a system, shall notify, as soon as practicable, the owner or licensee of the personal information of the breach of the security of a system.

(2) Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable, but not later than **[**45**]** **10** days after the business discovers or is notified of the breach of the security of a system.

(3) A business that is required to notify an owner or licensee of personal information of a breach of the security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach.

(4) (i) If the business that incurred the breach of the security of a system is not the owner or licensee of the computerized data, the business may not charge the owner or licensee of the computerized data a fee for providing information that the owner or licensee needs to make a notification under subsection (b)(2) of this section.

(ii) The owner or licensee of the computerized data may not use information relative to the breach of the security of a system for purposes other than:

1. Providing notification of the breach;

2. Protecting or securing personal information; or

3. Providing notification to national information security organizations created for information–sharing and analysis of security threats, to alert and avert new or expanded breaches.

(d) (1) The notification required under subsections (b) and (c) of this section may be delayed:

(i) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or

(ii) To determine the scope of the breach of the security of a system,

identify the individuals affected, or restore the integrity of the system.

(2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable, but not later than **[**30**]** **3** days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.

(e) The notification required under subsection (b) of this section **[**may**]** **SHALL** be given:

(1) By written notice sent to the most recent address of the individual in the records of the business;

(2) By electronic mail to the most recent electronic mail address of the individual in the records of the business, if:

(i) The individual has expressly consented to receive electronic notice; or

(ii) The business conducts its business primarily through Internet account transactions or the Internet; **OR**

(3) By telephonic notice, to the most recent telephone number of the individual in the records of the business**[**; or

(4) By substitute notice as provided in subsection (f) of this section, if:

(i) The business demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000; or

(ii) The business does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this subsection**]**.

(f) **[**Substitute notice under subsection (e)(4) of this section shall consist of**]** **THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION SHALL ALSO BE GIVEN BY**:

(1) Electronically mailing the notice to an individual entitled to notification under subsection (b) of this section, if the business has an electronic mail address for the individual to be notified;

(2) Conspicuous posting of the notice on the website of the business, if the business maintains a website; and

(3) Notification to **[**statewide media**]** **MAJOR MEDIA OUTLETS**

THROUGHOUT THE STATE.

(g) Except as provided in subsection (i) of this section, the notification required under subsection (b) of this section shall include:

(1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(2) Contact information for the business making the notification, including the business' address, telephone number, and toll–free telephone number if one is maintained;

(3) The toll–free telephone numbers and addresses for the major consumer reporting agencies; and

(4) (i) The toll–free telephone numbers, addresses, and website addresses for:

1. The Federal Trade Commission; and

2. The Office of the Attorney General; and

(ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

(h) **(1)** Prior to giving the notification required under subsection (b) of this section and subject to subsection (d) of this section, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.

(2) THE NOTICE REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL INCLUDE, AT A MINIMUM:

(I) THE NUMBER OF AFFECTED INDIVIDUALS RESIDING IN THE STATE;

(II) A DESCRIPTION OF THE BREACH OF THE SECURITY OF A SYSTEM, INCLUDING HOW IT OCCURRED AND ANY VULNERABILITIES THAT WERE EXPLOITED;

(III) ANY STEPS THE BUSINESS HAS TAKEN OR PLANS TO TAKE RELATING TO THE BREACH OF THE SECURITY OF A SYSTEM; AND

(IV) A SAMPLE OF EACH FORM OF NOTICE THAT WILL BE SENT TO CONSUMERS UNDER SUBSECTIONS (E) AND (F) OF THIS SECTION.

(i) (1) In the case of a breach of the security of a system involving personal information that permits access to an individual's e–mail account under § 14–3501(e)(1)(ii) of this subtitle and no other personal information under § 14–3501(e)(1)(i) of this subtitle, the business may comply with the notification requirement under subsection (b) of this section by providing the notification in electronic or other form that directs the individual whose personal information has been breached promptly to:

(i) Change the individual's password and security question or answer, as applicable; or

(ii) Take other steps appropriate to protect the e–mail account with the business and all other online accounts for which the individual uses the same user name or e–mail and password or security question or answer.

(2) Subject to paragraph (3) of this subsection, the notification provided under paragraph (1) of this subsection may be given to the individual by any method described in this section.

(3) (i) Except as provided in subparagraph (ii) of this paragraph, the notification provided under paragraph (1) of this subsection may not be given to the individual by sending notification by e–mail to the e–mail account affected by the breach.

(ii) The notification provided under paragraph (1) of this subsection may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected e–mail account from an Internet Protocol address or online location from which the business knows the individual customarily accesses the account.

(j) A waiver of any provision of this section is contrary to public policy and is void and unenforceable.

(k) Compliance with this section does not relieve a business from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2020.