

SENATE BILL 643

I3

2lr2674
CF 2lr2679

By: **Senators Lee, Feldman, and Benson**
Introduced and read first time: February 3, 2022
Assigned to: Finance

A BILL ENTITLED

1 AN ACT concerning

2 **Commercial Law – Maryland Personal Information Protection Act – Revisions**

3 FOR the purpose of requiring a business that maintains personal information of an
4 individual residing in the State to implement and maintain certain security
5 procedures and practices; altering certain requirements related to notifications of
6 breaches of the security of systems, including the circumstances under which the
7 owner or licensee of certain computerized data is required to notify certain
8 individuals of a breach; and generally relating to personal information and the
9 Maryland Personal Information Protection Act.

10 BY repealing and reenacting, with amendments,
11 Article – Commercial Law
12 Section 14–3501, 14–3503(a), and 14–3504
13 Annotated Code of Maryland
14 (2013 Replacement Volume and 2021 Supplement)

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

17 **Article – Commercial Law**

18 14–3501.

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

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

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

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



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

4 (D) “GENETIC TEST” MEANS AN ANALYSIS OF HUMAN DNA, RNA,
5 CHROMOSOMES, PROTEINS, OR METABOLITES.

6 [(d)] (E) “Health information” means any information [created by an entity
7 covered by the federal Health Insurance Portability and Accountability Act of 1996]
8 regarding an individual’s medical history, medical condition, or medical treatment or
9 diagnosis.

10 [(e)] (F) (1) “Personal information” means:

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

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

18 2. A driver’s license number or State identification card
19 number;

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

23 4. Health information, including information about an
24 individual’s mental health;

25 5. A health insurance policy or certificate number or health
26 insurance subscriber identification number, in combination with a unique identifier used
27 by an insurer or an employer that is self-insured, that permits access to an individual’s
28 health information; or

29 6. Biometric data of an individual generated by automatic
30 measurements of an individual’s biological characteristics such as a fingerprint, voice print,
31 genetic print, retina or iris image, or other unique biological characteristic, that can be used
32 to uniquely authenticate the individual’s identity when the individual accesses a system or
33 account; [or]

34 (ii) A user name or e-mail address in combination with a password

1 or security question and answer that permits access to an individual's e-mail account; **OR**

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

4 **1. THE GENETIC SAMPLE OF AN INDIVIDUAL;**

5 **2. A GENETIC TEST OF AN INDIVIDUAL;**

6 **3. A GENETIC TEST OF A FAMILY MEMBER OF AN**
7 **INDIVIDUAL;**

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

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

12 **6. ANY INFORMATION DERIVED FROM GENETIC**
13 **INFORMATION WITH RESPECT TO AN INDIVIDUAL.**

14 (2) "Personal information" does not include:

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

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

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

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

23 14-3503.

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

30 14-3504.

1 (a) In this section:

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

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

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

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

19 (3) Except as provided in subsection (d) of this section, the notification
20 required under paragraph (2) of this subsection shall be given as soon as reasonably
21 practicable, but not later than 45 days after the business [concludes the investigation
22 required under paragraph (1) of this subsection] **DISCOVERS OR IS NOTIFIED OF THE**
23 **BREACH OF THE SECURITY OF A SYSTEM.**

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

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

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

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

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

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

10 1. Providing notification of the breach;

11 2. Protecting or securing personal information; or

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

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

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

19 (ii) To determine the scope of the breach of the security of a system,
20 identify the individuals affected, or restore the integrity of the system.

21 (2) If notification is delayed under paragraph (1)(i) of this subsection,
22 notification shall be given as soon as reasonably practicable, but not later than [30] 7 days
23 after the law enforcement agency determines that it will not impede a criminal
24 investigation and will not jeopardize homeland or national security.

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

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

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

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

33 (ii) The business conducts its business primarily through Internet

1 account transactions or the Internet;

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

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

5 (i) The business demonstrates that the cost of providing notice
6 would exceed \$100,000 or that the affected class of individuals to be notified exceeds
7 175,000; or

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

10 (f) Substitute notice under subsection (e)(4) of this section shall consist of:

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

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

16 (3) Notification to [statewide media] **MAJOR PRINT OR BROADCAST**
17 **MEDIA IN GEOGRAPHIC AREAS WHERE THE INDIVIDUALS AFFECTED BY THE BREACH**
18 **LIKELY RESIDE.**

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

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

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

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

30 (4) (i) The toll-free telephone numbers, addresses, and website
31 addresses for:

32 1. The Federal Trade Commission; and

1 2. The Office of the Attorney General; and

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

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

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

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

11 **(II) A DESCRIPTION OF THE BREACH OF THE SECURITY OF A**
12 **SYSTEM, INCLUDING WHEN AND HOW IT OCCURRED;**

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

15 **(IV) THE FORM OF NOTICE THAT WILL BE SENT TO AFFECTED**
16 **INDIVIDUALS AND A SAMPLE NOTICE.**

17 (i) (1) In the case of a breach of the security of a system involving personal
18 information that permits access to an individual's e-mail account under §
19 [14-3501(e)(1)(ii)] **14-3501(F)(1)(II)** of this subtitle and no other personal information
20 under § [14-3501(e)(1)(i)] **14-3501(F)(1)(I)** of this subtitle, the business may comply with
21 the notification requirement under subsection (b) of this section by providing the
22 notification in electronic or other form that directs the individual whose personal
23 information has been breached promptly to:

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

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

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

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

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

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

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

11 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
12 October 1, 2022.