

HOUSE BILL 148

I3

(PRE-FILED)

1lr1047
CF SB 112

By: Delegate Carey

Requested: October 20, 2020

Introduced and read first time: January 13, 2021

Assigned to: Economic Matters

A BILL ENTITLED

1 AN ACT concerning

2 **Commercial Law – 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 the circumstances under which the owner or
6 licensee of certain computerized data is required to notify certain individuals of a
7 certain breach; altering the time periods within which certain notifications regarding
8 the breach of a security system are required to be given; requiring, rather than
9 authorizing, a certain notification to be given in a certain manner under certain
10 circumstances; requiring certain supplemental notifications to be provided in a
11 certain manner; requiring the notice of a certain breach provided to the Office of the
12 Attorney General to include certain information; defining a certain term and altering
13 a certain definition; and generally relating to personal information protection.

14 BY repealing and reenacting, with amendments,

15 Article – Commercial Law

16 Section 14–3501, 14–3503(a), and 14–3504

17 Annotated Code of Maryland

18 (2013 Replacement Volume and 2020 Supplement)

19 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,

20 That the Laws of Maryland read as follows:

21 **Article – Commercial Law**

22 14–3501.

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

24 (b) (1) “Business” means a sole proprietorship, partnership, corporation,

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 association, or any other business entity, whether or not organized to operate at a profit.

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

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

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

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

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

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

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

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

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

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

29 5. A health insurance policy or certificate number or health
30 insurance subscriber identification number, in combination with a unique identifier used
31 by an insurer or an employer that is self-insured, that permits access to an individual's
32 health information; or

33 6. Biometric data of an individual generated by automatic
34 measurements of an individual's biological characteristics such as a fingerprint, voice print,
35 genetic print, retina or iris image, or other unique biological characteristic, that can be used

1 to uniquely authenticate the individual's identity when the individual accesses a system or
2 account; [or]

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

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

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

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

9 **3. A GENETIC TEST OF A FAMILY MEMBER OF AN**
10 **INDIVIDUAL;**

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

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

15 **6. ANY INFORMATION DERIVED FROM GENETIC**
16 **INFORMATION WITH RESPECT TO AN INDIVIDUAL.**

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

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

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

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

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

26 14–3503.

27 (a) To protect personal information from unauthorized access, use, modification,
28 or disclosure, a business that owns, MAINTAINS, or licenses personal information of an
29 individual residing in the State shall implement and maintain reasonable security
30 procedures and practices that are appropriate to the nature of the personal information

1 owned, MAINTAINED, or licensed and the nature and size of the business and its
2 operations.

3 14–3504.

4 (a) In this section:

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

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

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

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

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

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

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

36 (2) Except as provided in subsection (d) of this section, the notification

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

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

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

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

13 1. Providing notification of the breach;

14 2. Protecting or securing personal information; or

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

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

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

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

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

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

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

32 (2) By electronic mail to the most recent electronic mail address of the
33 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;

(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:

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

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

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

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

33 (3) The toll-free telephone numbers and addresses for the major consumer

1 reporting agencies; and

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

4 1. The Federal Trade Commission; and

5 2. The Office of the Attorney General; and

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

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

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

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

15 (II) A DESCRIPTION OF THE BREACH OF THE SECURITY OF A
16 SYSTEM, INCLUDING WHEN AND HOW IT OCCURRED;

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

19 (IV) THE FORM OF NOTICE THAT WILL BE SENT TO AFFECTED
20 INDIVIDUALS AND A SAMPLE NOTICE.

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

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

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

HOUSE BILL 148

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

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

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

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

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

17 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
18 October 1, 2021.