

HOUSE BILL 1154

I3

9lr0810
CF SB 693

By: **Delegates Howard, Buckel, Chisholm, Malone, and Saab**

Introduced and read first time: February 8, 2019

Assigned to: Economic Matters

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 13, 2019

CHAPTER _____

1 AN ACT concerning

2 **Maryland Personal Information Protection Act – Security Breach Notification**
3 **Requirements – Modifications**

4 FOR the purpose of altering the applicability of certain security breach investigation
5 requirements to certain businesses; altering the applicability of certain security
6 breach notification requirements to a certain owner or licensee of computerized data;
7 prohibiting a certain business from charging a certain owner or licensee of
8 computerized data a fee for providing information that the owner or licensee needs
9 to provide a certain notification; prohibiting a certain owner or licensee from using
10 certain information for certain purposes; and generally relating to the Maryland
11 Personal Information Protection Act.

12 BY repealing and reenacting, with amendments,
13 Article – Commercial Law
14 Section 14–3504
15 Annotated Code of Maryland
16 (2013 Replacement Volume and 2018 Supplement)

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

19 **Article – Commercial Law**

20 14–3504.

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

Underlining indicates amendments to bill.

~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.



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 [or], licenses, **OR MAINTAINS** computerized data
10 that includes personal information of an individual residing in the State, when it discovers
11 or is notified [of] **THAT IT INCURRED** a breach of the security of a system, shall conduct in
12 good faith a reasonable and prompt investigation to determine the likelihood that personal
13 information of the individual has been or will be misused as a result of the breach.

14 (2) **[If] SUBJECT TO SUBSECTION (C)(4) OF THIS SECTION, IF**, after the
15 investigation is concluded, the business determines that the breach of the security of the
16 system creates a likelihood that personal information has been or will be misused, the
17 **[business] OWNER OR LICENSEE OF THE COMPUTERIZED DATA** shall notify the
18 individual 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.

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

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

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

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

1 (4) (I) IF THE BUSINESS THAT INCURRED THE BREACH OF THE
2 SECURITY OF A SYSTEM IS NOT THE OWNER OR LICENSEE OF THE COMPUTERIZED
3 DATA, THE BUSINESS MAY NOT CHARGE THE OWNER OR LICENSEE OF THE
4 COMPUTERIZED DATA A FEE FOR PROVIDING INFORMATION THAT THE OWNER OR
5 LICENSEE NEEDS TO MAKE A NOTIFICATION UNDER SUBSECTION (B)(2) OF THIS
6 SECTION.

7 (II) THE OWNER OR LICENSEE OF THE COMPUTERIZED DATA
8 MAY NOT USE INFORMATION RELATIVE TO THE BREACH OF THE SECURITY OF A
9 SYSTEM FOR PURPOSES OTHER THAN ~~PROVIDING~~:

10 1. ~~PROVIDING~~ NOTIFICATION OF THE BREACH ~~OR~~
11 ~~PROTECTING~~;

12 2. ~~PROTECTING~~ OR SECURING PERSONAL
13 INFORMATION; OR

14 3. PROVIDING NOTIFICATION TO NATIONAL
15 INFORMATION SECURITY ORGANIZATIONS CREATED FOR INFORMATION-SHARING
16 AND ANALYSIS OF SECURITY THREATS, TO ALERT AND AVERT NEW OR EXPANDED
17 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 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 be given:

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

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

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

3 (ii) The business conducts its business primarily through Internet
4 account transactions or the Internet;

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

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

8 (i) The business demonstrates that the cost of providing notice
9 would exceed \$100,000 or that the affected class of individuals to be notified exceeds
10 175,000; or

11 (ii) The business does not have sufficient contact information to give
12 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:

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

17 (2) Conspicuous posting of the notice on the [Web site] WEBSITE of the
18 business, if the business maintains a [Web site] WEBSITE; and

19 (3) Notification to statewide media.

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

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

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

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

31 (4) (i) The toll-free telephone numbers, addresses, and [Web site]
32 WEBSITE addresses for:

- 1 1. The Federal Trade Commission; and
- 2 2. The Office of the Attorney General; and

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

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

8 (i) (1) In the case of a breach of the security of a system involving personal
9 information that permits access to an individual's e-mail account under §
10 14-3501(e)(1)(ii) of this subtitle and no other personal information under § 14-3501(e)(1)(i)
11 of this subtitle, the business may comply with the notification requirement under
12 subsection (b) of this section by providing the notification in electronic or other form that
13 directs the individual whose personal information has been breached promptly to:

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

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

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

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

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

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

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

1 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
2 October 1, 2019.

Approved:

Governor.

Speaker of the House of Delegates.

President of the Senate.