

SENATE BILL 693

I3

9lr2131
CF 9lr0810

By: **Senators Kramer, Feldman, Hayes, Hershey, Jennings, and Kelley**

Introduced and read first time: February 4, 2019

Assigned to: Finance

A BILL ENTITLED

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.

21 (a) In this section:

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

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



(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 [or], licenses, **OR MAINTAINS** computerized data that includes personal information of an individual residing in the State, when it discovers or is notified [of] **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) **[If] SUBJECT TO SUBSECTION (C)(4) OF THIS SECTION, IF**, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the **[business] 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 days after the business concludes the investigation required under paragraph (1) of this subsection.

(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 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**

1 LICENSEE NEEDS TO MAKE A NOTIFICATION UNDER SUBSECTION (B)(2) OF THIS
2 SECTION.

3 (II) THE OWNER OR LICENSEE OF THE COMPUTERIZED DATA
4 MAY NOT USE INFORMATION RELATIVE TO THE BREACH OF THE SECURITY OF A
5 SYSTEM FOR PURPOSES OTHER THAN PROVIDING NOTIFICATION OF THE BREACH OR
6 PROTECTING OR SECURING PERSONAL INFORMATION.

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

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

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

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

17 (e) The notification required under subsection (b) of this section may be given:

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

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

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

24 (ii) The business conducts its business primarily through Internet
25 account transactions or the Internet;

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

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

29 (i) The business demonstrates that the cost of providing notice
30 would exceed \$100,000 or that the affected class of individuals to be notified exceeds
31 175,000; or

32 (ii) The business does not have sufficient contact information to give

1 notice in accordance with item (1), (2), or (3) of this subsection.

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

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

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

8 (3) Notification to statewide media.

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

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

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

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

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

22 1. The Federal Trade Commission; and

23 2. The Office of the Attorney General; and

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

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

29 (i) (1) In the case of a breach of the security of a system involving personal
30 information that permits access to an individual's e-mail account under §
31 14-3501(e)(1)(ii) of this subtitle and no other personal information under § 14-3501(e)(1)(i)
32 of this subtitle, the business may comply with the notification requirement under
33 subsection (b) of this section by providing the notification in electronic or other form that

1 directs the individual whose personal information has been breached promptly to:

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

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

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

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

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

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

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

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