

HOUSE BILL 1584

I3

8lr2999
CF 8lr3422

By: **Delegates S. Howard, Chang, Clark, Rose, Saab, and Shoemaker**

Introduced and read first time: February 9, 2018

Assigned to: Economic Matters

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 18, 2018

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 and
5 notification requirements to certain businesses; prohibiting a certain business from
6 charging a certain owner or licensee of computerized data a fee for providing
7 information that the owner or licensee needs to provide a certain notification;
8 prohibiting a certain owner or licensee from using certain information for certain
9 purposes; altering the authorized methods of providing a certain notification;
10 requiring the Office of the Attorney General to post a certain notice of a breach on
11 the website of the Office of the Attorney General; and generally relating to the
12 Maryland Personal Information Protection Act.

13 BY repealing and reenacting, with amendments,
14 Article – Commercial Law
15 Section 14–3504
16 Annotated Code of Maryland
17 (2013 Replacement Volume and 2017 Supplement)

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

20 **Article – Commercial Law**

21 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 shall notify the individual of the breach.

18 (3) Except as provided in subsection (d) of this section, the notification
19 required under paragraph (2) of this subsection shall be given as soon as reasonably
20 practicable, but not later than 45 days after the business concludes the investigation
21 required under paragraph (1) of this subsection.

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

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

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

35 (3) A business that is required to notify an owner or licensee of personal
36 information of a breach of the security of a system under paragraph (1) of this subsection
37 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 NOTIFICATION OF THE BREACH OR**
10 **PROTECTING OR SECURING PERSONAL INFORMATION.**

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

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

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

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

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

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

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

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

28 (ii) The business conducts its business primarily through Internet
29 account transactions or the Internet;

30 (3) By telephonic notice, to the most recent telephone number of the
31 individual in the records of the business; ~~for~~

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

1 (i) The business demonstrates that the cost of providing notice
2 would exceed \$100,000 or that the affected class of individuals to be notified exceeds
3 175,000; or

4 (ii) The business does not have sufficient contact information to give
5 notice in accordance with item (1), (2), or (3) of this subsection~~1~~;

6 ~~(4)~~ (5) BY CONSPICUOUS POSTING OF THE NOTICE ON THE
7 WEBSITE OF THE BUSINESS, IF THE BUSINESS MAINTAINS A WEBSITE; OR

8 ~~(5)~~ (6) BY NOTIFICATION TO STATEWIDE MEDIA; ~~OR~~

9 ~~(6)~~ ~~BY CONSPICUOUS POSTING OF A NOTICE AT THE BUSINESS'S~~
10 ~~PLACE OF BUSINESS.~~

11 (f) ~~1~~ Substitute notice under subsection (e)(4) of this section shall consist of:

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

15 (2) Conspicuous posting of the notice on the ~~Web site~~ WEBSITE of the
16 business, if the business maintains a ~~Web site~~ WEBSITE; and

17 (3) Notification to statewide media.

18 (g)~~1~~ Except as provided in subsection ~~[(i)]~~ ~~(H)~~ of this section, the notification
19 required under subsection (b) of this section shall include:

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

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

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

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

31 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)]~~ ~~(G)~~ (1) Prior to giving the notification required under subsection (b) of
5 this 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) **AFTER RECEIVING NOTICE OF A BREACH OF A SECURITY SYSTEM**
8 **FROM A BUSINESS, THE OFFICE OF THE ATTORNEY GENERAL SHALL POST A NOTICE**
9 **OF THE BREACH ON THE WEBSITE OF THE OFFICE OF THE ATTORNEY GENERAL.**

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

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

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

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

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

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

32 ~~[(j)]~~ ~~(I)~~ A waiver of any provision of this section is contrary to public policy and
33 is void and unenforceable.

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

4 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
5 October 1, 2018.

Approved:

Governor.

Speaker of the House of Delegates.

President of the Senate.