

SENATE BILL 552

I3

7lr2647
CF 7lr1032

By: **Senator Hershey**

Introduced and read first time: February 1, 2017

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 and
5 notification requirements to certain businesses; authorizing a certain business to
6 elect to provide a certain notification; prohibiting a certain business from requiring
7 or compelling a certain business to make a certain election; altering the provisions
8 of law with which certain businesses and affiliates shall be deemed to be in
9 compliance by being subject to and in compliance with certain federal laws and
10 guidelines; and generally relating to the Maryland Personal Information Protection
11 Act.

12 BY repealing and reenacting, without amendments,
13 Article – Commercial Law
14 Section 14–3504(a)
15 Annotated Code of Maryland
16 (2013 Replacement Volume and 2016 Supplement)

17 BY repealing and reenacting, with amendments,
18 Article – Commercial Law
19 Section 14–3504(b) and (c) and 14–3507
20 Annotated Code of Maryland
21 (2013 Replacement Volume and 2016 Supplement)

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

24 **Article – Commercial Law**

25 14–3504.

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



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] **MAINTAINS** computerized data that
10 includes personal information of an individual residing in the State, when it discovers or is
11 notified [of] **THAT IT INCURRED** a breach of the security of a system, shall conduct in good
12 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, after the investigation is concluded, the business determines that
15 misuse of the individual's personal information has occurred or is reasonably likely to occur
16 as a result of a breach of the security of a system, the business shall notify the individual
17 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 after the business conducts the investigation required under paragraph (1) of
21 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 that the business does not own or license shall notify the owner or licensee of
28 the personal information of a breach of the security of a system if it is likely that the breach
29 has resulted or will result in the misuse of personal information of an individual residing
30 in the State.

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 after the business discovers or is notified of the breach of the security of a
34 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) AFTER RECEIPT OF THE NOTIFICATION REQUIRED UNDER**
2 **PARAGRAPH (1) OF THIS SUBSECTION, THE BUSINESS THAT OWNS OR LICENSES THE**
3 **COMPUTERIZED DATA MAY ELECT TO PROVIDE ON BEHALF OF THE BUSINESS THAT**
4 **INCURRED THE BREACH OF THE SECURITY OF A SYSTEM ANY NOTIFICATION TO AN**
5 **INDIVIDUAL REQUIRED UNDER SUBSECTION (B)(2) OF THIS SECTION.**

6 **(5) THE BUSINESS THAT INCURRED THE BREACH OF THE SECURITY**
7 **OF A SYSTEM MAY NOT REQUIRE OR COMPEL A BUSINESS THAT OWNS OR LICENSES**
8 **THE COMPUTERIZED DATA TO MAKE THE ELECTION UNDER PARAGRAPH (4) OF THIS**
9 **SUBSECTION.**

10 14–3507.

11 (a) In this section, “affiliate” means a company that controls, is controlled by, or
12 is under common control with a business described in subsection (c)(1) of this section.

13 (b) A business that complies with the requirements for notification procedures,
14 the protection or security of personal information, or the destruction of personal
15 information under the rules, regulations, procedures, or guidelines established by the
16 primary or functional federal or State regulator of the business shall be deemed to be in
17 compliance with this subtitle.

18 (c) (1) A business that is subject to and in compliance with § 501(b) of the
19 federal Gramm–Leach–Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate
20 Credit Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines
21 Establishing Information Security Standards, and the federal Interagency Guidance on
22 Response Programs for Unauthorized Access to Customer Information and Customer
23 Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance
24 with **§ 14–3503 OF** this subtitle.

25 (2) An affiliate that complies with § 501(b) of the federal
26 Gramm–Leach–Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit
27 Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines Establishing
28 Information Security Standards, and the federal Interagency Guidance on Response
29 Programs for Unauthorized Access to Customer Information and Customer Notice, and any
30 revisions, additions, or substitutions, shall be deemed to be in compliance with **§ 14–3503**
31 **OF** this subtitle.

32 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
33 October 1, 2017.