

SENATE BILL 525

I3

7lr0332
CF HB 974

By: **Senators Lee, Benson, Feldman, Kagan, Kelley, King, Madaleno, Manno, Nathan-Pulliam, Peters, Pinsky, Robinson, Rosapepe, Smith, Young, and Zucker**

Introduced and read first time: February 1, 2017
Assigned to: Finance

Committee Report: Favorable with amendments
Senate action: Adopted
Read second time: March 31, 2017

CHAPTER _____

1 AN ACT concerning

2 **Maryland Personal Information Protection Act – Revisions**

3 FOR the purpose of requiring a certain business, when destroying an employee's or a former
4 employee's records that contain certain personal information of the employee or
5 former employee, to take certain steps to protect against unauthorized access to or
6 use of the information; altering the circumstances under which a certain business
7 that owns, licenses, or maintains computerized data that includes certain personal
8 information of an individual residing in the State must conduct a certain
9 investigation and notify certain persons of a breach of the security of a system;
10 specifying the time at which certain notice must be given; authorizing a certain
11 business to provide a certain required notice in a certain manner under certain
12 circumstances; providing that a certain business and a certain affiliate that comply
13 with a certain federal law shall be deemed to be in compliance with certain provisions
14 of law; defining a certain term; altering certain definitions; providing for a delayed
15 effective date; and generally relating to the protection of personal information
16 contained in the records of businesses, owned or licensed by businesses, or included
17 in computerized data owned, licensed, or maintained by businesses.

18 BY repealing and reenacting, with amendments,
19 Article – Commercial Law
20 Section 14-3501, 14-3502, 14-3504, and ~~14-3506~~ 14-3507
21 Annotated Code of Maryland
22 (2013 Replacement Volume and 2016 Supplement)

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 BY repealing and reenacting, without amendments,
 2 Article – Commercial Law
 3 Section 14–3503, 14–3505, ~~14–3507~~ 14–3506, and 14–3508
 4 Annotated Code of Maryland
 5 (2013 Replacement Volume and 2016 Supplement)

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

8 **Article – Commercial Law**

9 14–3501.

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

11 (b) (1) “Business” means a sole proprietorship, partnership, corporation,
 12 association, or any other business entity, whether or not organized to operate at a profit.

13 (2) “Business” includes a financial institution organized, chartered,
 14 licensed, or otherwise authorized under the laws of this State, any other state, the United
 15 States, or any other country, and the parent or subsidiary of a financial institution.

16 (c) “Encrypted” means the [transformation of data through the use of an
 17 algorithmic process into a form in which there is a low probability of assigning meaning
 18 without use of a confidential process or key] **PROTECTION OF DATA IN ELECTRONIC OR
 19 OPTICAL FORM, IN STORAGE OR IN TRANSIT, USING AN ENCRYPTION TECHNOLOGY
 20 THAT:**

21 ~~(1) HAS BEEN ADOPTED BY AN ESTABLISHED STANDARDS SETTING
 22 BODY OF THE FEDERAL GOVERNMENT, INCLUDING THE FEDERAL INFORMATION
 23 PROCESSING STANDARDS ISSUED BY THE NATIONAL INSTITUTE OF STANDARDS
 24 AND TECHNOLOGY; AND~~

25 ~~(2) RENDERS RENDERS~~ **RENDERS** THE DATA INDECIPHERABLE WITHOUT AN
 26 ASSOCIATED CRYPTOGRAPHIC KEY NECESSARY TO ENABLE DECRYPTION OF THE
 27 DATA.

28 **(D) “HEALTH INFORMATION” MEANS ANY INFORMATION CREATED BY AN
 29 ENTITY COVERED BY THE FEDERAL HEALTH INSURANCE PORTABILITY AND
 30 ACCOUNTABILITY ACT OF 1996 REGARDING AN INDIVIDUAL’S MEDICAL HISTORY,
 31 MEDICAL CONDITION, OR MEDICAL TREATMENT OR DIAGNOSIS.**

32 ~~(d)~~ **(E)** (1) “Personal information” means ~~an~~:

1 **(I)** AN individual's first name or first initial and last name in
 2 combination with any one or more of the following data elements, when the name or the
 3 data elements are not encrypted, redacted, or otherwise protected by another method that
 4 renders the information unreadable or unusable:

5 ~~(i)~~ **1.** A Social Security number, **AN INDIVIDUAL TAXPAYER**
 6 **IDENTIFICATION NUMBER, A PASSPORT NUMBER, OR OTHER IDENTIFICATION**
 7 **NUMBER ISSUED BY THE FEDERAL GOVERNMENT;**

8 ~~(ii)~~ **2.** A driver's license number **OR STATE IDENTIFICATION**
 9 **CARD NUMBER;**

10 ~~(iii)~~ **3.** ~~A financial~~ AN account number, ~~including~~ a credit card
 11 number, or A debit card number, ~~that~~ in combination with any required security code,
 12 access code, or password, ~~would permit~~ **THAT PERMITS** access to an individual's financial
 13 account; [or]

14 ~~(iv)~~ **4.** [An Individual Taxpayer Identification Number]
 15 **MEDICAL HEALTH** INFORMATION, INCLUDING INFORMATION ABOUT AN
 16 INDIVIDUAL'S MENTAL HEALTH;

17 ~~(v)~~ **5.** A HEALTH INSURANCE POLICY OR CERTIFICATE
 18 NUMBER OR HEALTH INSURANCE SUBSCRIBER IDENTIFICATION NUMBER THAT, IN
 19 COMBINATION WITH A UNIQUE IDENTIFIER USED BY AN INSURER OR AN EMPLOYER
 20 THAT IS SELF-INSURED, WOULD PERMIT THAT PERMITS ACCESS TO AN
 21 INDIVIDUAL'S MEDICAL HEALTH INFORMATION; OR

22 ~~(vi)~~ ~~A USER NAME OR E-MAIL ADDRESS THAT, IN COMBINATION~~
 23 ~~WITH A PASSWORD OR SECURITY QUESTION AND ANSWER, WOULD PERMIT ACCESS~~
 24 ~~TO AN INDIVIDUAL'S ONLINE ACCOUNT; OR~~

25 ~~(vii)~~ **6.** ~~ANY BIOMETRIC~~ BIOMETRIC DATA OF AN
 26 INDIVIDUAL, ~~INCLUDING~~ GENERATED BY AUTOMATIC MEASUREMENTS OF AN
 27 INDIVIDUAL'S BIOLOGICAL CHARACTERISTICS SUCH AS A FINGERPRINT, VOICE
 28 PRINT, GENETIC PRINT, OR RETINA OR IRIS IMAGE, OR OTHER UNIQUE BIOLOGICAL
 29 CHARACTERISTIC, THAT CAN BE USED TO IDENTIFY THE INDIVIDUAL UNIQUELY
 30 AUTHENTICATE THE INDIVIDUAL'S IDENTITY WHEN THE INDIVIDUAL ACCESSES A
 31 SYSTEM OR ACCOUNT; OR

32 **(II)** A USER NAME OR E-MAIL ADDRESS IN COMBINATION WITH
 33 A PASSWORD OR SECURITY QUESTION AND ANSWER THAT PERMITS ACCESS TO AN
 34 INDIVIDUAL'S E-MAIL ACCOUNT.

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

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

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

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

7 ~~(E) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS DATA~~
8 ~~SECURITY PROCEDURES AND PRACTICES DEVELOPED IN GOOD FAITH AND SET~~
9 ~~FORTH IN A WRITTEN INFORMATION SECURITY POLICY THAT CLEARLY~~
10 ~~DEMONSTRATES THAT THE PROCEDURES AND PRACTICES;~~

11 ~~(1) COORDINATE AN INFORMATION SECURITY PROGRAM;~~

12 ~~(2) REQUIRE A RISK ASSESSMENT TO IDENTIFY REASONABLY~~
13 ~~FORESEEABLE INTERNAL AND EXTERNAL RISKS TO THE SECURITY,~~
14 ~~CONFIDENTIALITY, AND INTEGRITY OF PERSONAL INFORMATION AND TO ASSESS~~
15 ~~THE SUFFICIENCY OF ANY SAFEGUARDS IN PLACE TO CONTROL THE RISKS;~~

16 ~~(3) ONCE A RISK ASSESSMENT IS COMPLETED, INCLUDE DESIGN~~
17 ~~SAFEGUARDS TO CONTROL THE IDENTIFIED RISKS AND TO REGULARLY MONITOR~~
18 ~~THE EFFECTIVENESS OF THE CONTROLS;~~

19 ~~(4) ENSURE, IN ANY CONTRACT WITH A SERVICE PROVIDER, THAT~~
20 ~~THE SERVICE PROVIDER IS CAPABLE OF PROVIDING APPROPRIATE SAFEGUARDS~~
21 ~~FOR THE PERSONAL INFORMATION; AND~~

22 ~~(5) EVALUATE AND ADJUST THE INFORMATION SECURITY PROGRAM~~
23 ~~BASED ON:~~

24 ~~(I) THE FINDINGS OF THE REGULAR MONITORING AND~~
25 ~~TESTING OF INFORMATION SAFEGUARDS;~~

26 ~~(II) MATERIAL CHANGES TO OPERATIONS OR BUSINESS~~
27 ~~ARRANGEMENTS; OR~~

28 ~~(III) CIRCUMSTANCES THAT THE BUSINESS KNOWS OR HAS~~
29 ~~REASON TO KNOW MAY HAVE A MATERIAL IMPACT ON THE INFORMATION SECURITY~~
30 ~~PROGRAM OF THE BUSINESS.~~

31 [(e)] (F) "Records" means information that is inscribed on a tangible medium or
32 that is stored in an electronic or other medium and is retrievable in perceivable form.

1 14-3502.

2 (a) In this section, "customer" means an individual residing in the State who
3 provides personal information to a business for the purpose of purchasing or leasing a
4 product or obtaining a service from the business.

5 (b) When a business is destroying a customer's, **AN EMPLOYEE'S, OR A FORMER**
6 **EMPLOYEE'S** records that contain personal information of the customer, **EMPLOYEE, OR**
7 **FORMER EMPLOYEE**, the business shall take reasonable steps to protect against
8 unauthorized access to or use of the personal information, taking into account:

9 (1) The sensitivity of the records;

10 (2) The nature and size of the business and its operations;

11 (3) The costs and benefits of different destruction methods; and

12 (4) Available technology.

13 14-3503.

14 (a) To protect personal information from unauthorized access, use, modification,
15 or disclosure, a business that owns or licenses personal information of an individual
16 residing in the State shall implement and maintain reasonable security procedures and
17 practices that are appropriate to the nature of the personal information owned or licensed
18 and the nature and size of the business and its operations.

19 (b) (1) A business that uses a nonaffiliated third party as a service provider to
20 perform services for the business and discloses personal information about an individual
21 residing in the State under a written contract with the third party shall require by contract
22 that the third party implement and maintain reasonable security procedures and practices
23 that:

24 (i) Are appropriate to the nature of the personal information
25 disclosed to the nonaffiliated third party; and

26 (ii) Are reasonably designed to help protect the personal information
27 from unauthorized access, use, modification, disclosure, or destruction.

28 (2) This subsection shall apply to a written contract that is entered into on
29 or after January 1, 2009.

30 14-3504.

31 (a) In this section:

1 (1) "Breach of the security of a system" means the unauthorized
 2 ~~ACCESSING OR~~ acquisition of computerized data that compromises the security,
 3 confidentiality, or integrity of the personal information maintained by a business; and

4 (2) "Breach of the security of a system" does not include the good faith
 5 ~~ACCESSING OR~~ acquisition of personal information by an employee or agent of a business
 6 for the purposes of the business, provided that the personal information is not used or
 7 subject to further unauthorized disclosure.

8 (b) (1) A business that owns or licenses computerized data that includes
 9 personal information of an individual residing in the State, when it discovers or is notified
 10 of a breach of the security of a system, shall conduct in good faith a reasonable and prompt
 11 investigation to determine ~~[the likelihood that] WHETHER AN UNAUTHORIZED~~
 12 ~~ACCESSING OR ACQUISITION OF THE~~ personal information of the individual has ~~[been or~~
 13 will be misused as a result of the breach] ~~OCCURRED~~.

14 (2) If, after the investigation is concluded, the business determines that
 15 [misuse] ~~AN UNAUTHORIZED ACCESSING OR ACQUISITION~~ of the individual's personal
 16 ~~information has occurred or is reasonably likely to occur as a result of a breach of the~~
 17 ~~security of a system~~ THE BREACH OF THE SECURITY OF A SYSTEM CREATES A
 18 LIKELIHOOD THAT PERSONAL INFORMATION HAS BEEN OR WILL BE MISUSED, the
 19 business shall notify the individual of the breach.

20 (3) Except as provided in subsection (d) of this section, the notification
 21 required under paragraph (2) of this subsection shall be given as soon as reasonably
 22 practicable, **BUT NOT LATER THAN 30 45 DAYS** after the business [conducts]
 23 **CONCLUDES** the investigation required under paragraph (1) of this subsection.

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

28 (c) (1) A business that maintains computerized data that includes personal
 29 information OF AN INDIVIDUAL RESIDING IN THE STATE that the business does not own
 30 or license, WHEN IT DISCOVERS OR IS NOTIFIED OF A BREACH OF THE SECURITY OF A
 31 SYSTEM, shall notify, AS SOON AS PRACTICABLE, the owner or licensee of the personal
 32 information of a THE breach of the security of a system ~~if it is likely that the breach has~~
 33 ~~resulted or will result in the [misuse] ACCESSING OR ACQUISITION~~ of personal
 34 ~~information of an individual residing in the State.~~

35 (2) Except as provided in subsection (d) of this section, the notification
 36 required under paragraph (1) of this subsection shall be given as soon as reasonably
 37 practicable, **BUT NOT LATER THAN 30 45 DAYS** after the business discovers or is notified
 38 of the breach of the security of a system.

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

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

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

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

10 (2) If notification is delayed under paragraph (1)(i) of this subsection,
11 notification shall be given as soon as reasonably practicable, **BUT NOT LATER THAN 30**
12 **DAYS** after the law enforcement agency determines that it will not impede a criminal
13 investigation and will not jeopardize homeland or national security.

14 (e) The notification required under ~~subsections (b) and (c)~~ **SUBSECTION (B)** of
15 this section may be given:

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

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

20 (i) The individual has expressly consented to receive electronic
21 notice; or

22 (ii) The business conducts its business primarily through Internet
23 account transactions or the Internet;

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

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

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

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

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

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

4 (2) Conspicuous posting of the notice on the Web site of the business, if the
5 business maintains a Web site; and

6 (3) Notification to statewide media.

7 (g) ~~The~~ **EXCEPT AS PROVIDED IN SUBSECTION (I) OF THIS SECTION, THE**
8 notification required under subsection (b) of this section shall include:

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

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

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

18 (4) (i) The toll-free telephone numbers, addresses, and Web site
19 addresses for:

20 1. The Federal Trade Commission; and

21 2. The Office of the Attorney General; and

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

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

27 **(I) (1) IN THE CASE OF A BREACH OF THE SECURITY OF A SYSTEM**
28 **INVOLVING PERSONAL INFORMATION THAT PERMITS ACCESS TO AN INDIVIDUAL'S**
29 **E-MAIL ACCOUNT UNDER § 14-3501(E)(1)(II) OF THIS SUBTITLE AND NO OTHER**
30 **PERSONAL INFORMATION UNDER § 14-3501(E)(1)(I) OF THIS SUBTITLE, THE**
31 **BUSINESS MAY COMPLY WITH THE NOTIFICATION REQUIREMENT UNDER**
32 **SUBSECTION (B) OF THIS SECTION BY PROVIDING THE NOTIFICATION IN**
33 **ELECTRONIC OR OTHER FORM THAT DIRECTS THE INDIVIDUAL WHOSE PERSONAL**
34 **INFORMATION HAS BEEN BREACHED PROMPTLY TO:**

1 (I) CHANGE THE INDIVIDUAL'S PASSWORD AND SECURITY
2 QUESTION OR ANSWER, AS APPLICABLE; OR

3 (II) TAKE OTHER STEPS APPROPRIATE TO PROTECT THE
4 E-MAIL ACCOUNT WITH THE BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR
5 WHICH THE INDIVIDUAL USES THE SAME USER NAME OR E-MAIL AND PASSWORD OR
6 SECURITY QUESTION OR ANSWER.

7 (2) SUBJECT TO PARAGRAPH (3) OF THIS SUBSECTION, THE
8 NOTIFICATION PROVIDED UNDER PARAGRAPH (1) OF THIS SUBSECTION MAY BE
9 GIVEN TO THE INDIVIDUAL BY ANY METHOD DESCRIBED IN THIS SECTION.

10 (3) (I) EXCEPT AS PROVIDED IN SUBPARAGRAPH (II) OF THIS
11 PARAGRAPH, THE NOTIFICATION PROVIDED UNDER PARAGRAPH (1) OF THIS
12 SUBSECTION MAY NOT BE GIVEN TO THE INDIVIDUAL BY SENDING NOTIFICATION BY
13 E-MAIL TO THE E-MAIL ACCOUNT AFFECTED BY THE BREACH.

14 (II) THE NOTIFICATION PROVIDED UNDER PARAGRAPH (1) OF
15 THIS SUBSECTION MAY BE GIVEN BY A CLEAR AND CONSPICUOUS NOTICE
16 DELIVERED TO THE INDIVIDUAL ONLINE WHILE THE INDIVIDUAL IS CONNECTED TO
17 THE AFFECTED E-MAIL ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR
18 ONLINE LOCATION FROM WHICH THE BUSINESS KNOWS THE INDIVIDUAL
19 CUSTOMARILY ACCESSES THE ACCOUNT.

20 ~~(J)~~ (J) A waiver of any provision of this section is contrary to public policy and
21 is void and unenforceable.

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

25 14-3505.

26 The provisions of this subtitle are exclusive and shall preempt any provision of local
27 law.

28 14-3506.

29 (a) If a business is required under § 14-3504 of this subtitle to give notice of a
30 breach of the security of a system to 1,000 or more individuals, the business also shall
31 notify, ~~without unreasonable delay~~ ~~NOT LATER THAN 30 DAYS AFTER NOTICE OF A~~
32 ~~BREACH IS GIVEN TO INDIVIDUALS~~, each consumer reporting agency that compiles and
33 maintains files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a(p), of
34 the timing, distribution, and content of the notices.

1 (b) This section does not require the inclusion of the names or other personal
2 identifying information of recipients of notices of the breach of the security of a system.

3 14–3507.

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

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

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

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

25 **(D) (1) A BUSINESS THAT IS SUBJECT TO AND IN COMPLIANCE WITH THE**
26 **FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996**
27 **SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.**

28 **(2) AN AFFILIATE THAT IS IN COMPLIANCE WITH THE FEDERAL**
29 **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 SHALL BE**
30 **DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.**

31 14–3508.

32 A violation of this subtitle:

33 (1) Is an unfair or deceptive trade practice within the meaning of Title 13
34 of this article; and

1 (2) Is subject to the enforcement and penalty provisions contained in Title
2 13 of this article.

3 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
4 ~~October 1, 2017~~ January 1, 2018.

Approved:

Governor.

President of the Senate.

Speaker of the House of Delegates.