

HOUSE BILL 960

I3

3lr1607
CF SB 859

By: **Delegate Lee (Commission on Maryland Cybersecurity Innovation and Excellence) and Delegates Conaway, DeBoy, Dumais, Glenn, Hough, Kaiser, and B. Robinson**

Introduced and read first time: February 7, 2013

Assigned to: Economic Matters

A BILL ENTITLED

1 AN ACT concerning

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

3 FOR the purpose of requiring a certain business, when destroying a customer's records
4 that contain certain personal or private information of the customer, to take
5 certain steps to protect against unauthorized access to or use of the information;
6 requiring a certain business to implement and maintain certain procedures and
7 practices to protect against the unauthorized access, use, modification, or
8 disclosure of the personal or certain private information under certain
9 circumstances; requiring a certain business that owns or licenses computerized
10 data that includes certain personal or private information of an individual
11 residing in the State to implement and maintain certain security procedures
12 and practices under certain circumstances; altering the circumstances under
13 which a certain business that owns, licenses, or maintains computerized data
14 that includes certain private information of an individual residing in the State
15 must conduct a certain investigation and notify certain persons of a breach of
16 the security of a system; specifying the time at which certain notice must be
17 given; altering the contents of the notice; defining certain terms; altering
18 certain definitions; making certain conforming changes; providing for the
19 application of a certain provision of this Act; and generally relating to the
20 protection of personal or private information contained in the records of
21 businesses, owned or licensed by businesses, or included in computerized data
22 owned, licensed, or maintained by businesses.

23 BY repealing and reenacting, with amendments,
24 Article – Commercial Law
25 Section 14–3501 through 14–3504, 14–3506, and 14–3507
26 Annotated Code of Maryland
27 (2005 Replacement Volume and 2012 Supplement)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 BY repealing and reenacting, without amendments,
2 Article – Commercial Law
3 Section 14–3505 and 14–3508
4 Annotated Code of Maryland
5 (2005 Replacement Volume and 2012 Supplement)

6 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF
7 MARYLAND, 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
13 profit.

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

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

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

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

30 (d) (1) “Personal information” means [an individual’s first name or first
31 initial and last name in combination with any one or more of the following data
32 elements, when the name or the data elements are not encrypted, redacted, or
33 otherwise protected by another method that renders the information unreadable or
34 unusable:

35 (i) A Social Security number;

1 (ii) A driver's license number;

2 (iii) A financial account number, including a credit card number
3 or debit card number, that in combination with any required security code, access
4 code, or password, would permit access to an individual's financial account; or

5 (iv) An Individual Taxpayer Identification Number] ANY
6 INFORMATION RELATING TO AN INDIVIDUAL, INCLUDING NAME, NUMBER,
7 PERSONAL MARK, UNIQUE BIOMETRIC OR GENETIC PRINT, IMAGE, OR DATA, OR
8 ANY OTHER IDENTIFIER, THAT CAN BE USED TO IDENTIFY THE INDIVIDUAL.

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

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

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

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

16 (E) "PRIVATE INFORMATION" MEANS PERSONAL INFORMATION IN
17 COMBINATION WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS,
18 WHETHER OR NOT ANY OF THE ELEMENTS ARE ENCRYPTED:

19 (1) A SOCIAL SECURITY NUMBER;

20 (2) A DRIVER'S LICENSE NUMBER OR STATE IDENTIFICATION
21 CARD NUMBER;

22 (3) A PASSPORT NUMBER OR OTHER UNITED STATES ISSUED
23 IDENTIFICATION NUMBER; OR

24 (4) AN ACCOUNT NUMBER OR CREDIT OR DEBIT CARD NUMBER
25 THAT, IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE,
26 OR PASSWORD, WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL
27 ACCOUNT.

28 (F) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS
29 DATA SECURITY PROCEDURES AND PRACTICES DEVELOPED, IN GOOD FAITH,
30 AND SET FORTH IN A WRITTEN INFORMATION SECURITY POLICY THAT CLEARLY
31 DEMONSTRATES THAT THE PROCEDURES AND PRACTICES:

1 **(1) COORDINATE AN INFORMATION SECURITY PROGRAM;**

2 **(2) REQUIRE A RISK ASSESSMENT TO IDENTIFY REASONABLY**
3 **FORESEEABLE INTERNAL AND EXTERNAL RISKS TO THE SECURITY,**
4 **CONFIDENTIALITY, AND INTEGRITY OF CUSTOMER INFORMATION AND TO**
5 **ASSESS THE SUFFICIENCY OF ANY SAFEGUARDS IN PLACE TO CONTROL THE**
6 **RISKS;**

7 **(3) ONCE A RISK ASSESSMENT IS COMPLETED, INCLUDE DESIGN**
8 **SAFEGUARDS TO CONTROL THE IDENTIFIED RISKS AND TO REGULARLY**
9 **MONITOR THE EFFECTIVENESS OF THE CONTROLS;**

10 **(4) ENSURE, IN ANY CONTRACT WITH A SERVICE PROVIDER, THAT**
11 **THE SERVICE PROVIDER IS CAPABLE OF PROVIDING APPROPRIATE**
12 **SAFEGUARDS FOR THE PERSONAL INFORMATION AND PRIVATE INFORMATION**
13 **OF CUSTOMERS; AND**

14 **(5) EVALUATE AND ADJUST THE INFORMATION SECURITY**
15 **PROGRAM BASED ON:**

16 **(I) THE FINDINGS OF THE REGULAR MONITORING AND**
17 **TESTING OF INFORMATION SAFEGUARDS;**

18 **(II) MATERIAL CHANGES TO OPERATIONS OR BUSINESS**
19 **ARRANGEMENTS; OR**

20 **(III) CIRCUMSTANCES THAT THE BUSINESS KNOWS OR HAS**
21 **REASON TO KNOW MAY HAVE A MATERIAL IMPACT ON THE INFORMATION**
22 **SECURITY PROGRAM OF THE BUSINESS.**

23 **[(e)] (G) “Records” means information that is inscribed on a tangible**
24 **medium or that is stored in an electronic or other medium and is retrievable in**
25 **perceivable form.**

26 14–3502.

27 (a) In this section, “customer” means an individual residing in the State who
28 provides personal **INFORMATION OR PRIVATE** information to a business for the
29 purpose of purchasing or leasing a product or obtaining a service from the business.

30 (b) When a business is destroying a customer’s records that contain personal
31 **INFORMATION OR PRIVATE** information of the customer, the business shall take
32 reasonable steps to protect against unauthorized access to or use of the personal
33 **INFORMATION OR PRIVATE** information, taking into account:

- 1 (1) The sensitivity of the records;
- 2 (2) The nature and size of the business and its operations;
- 3 (3) The costs and benefits of different destruction methods; and
- 4 (4) Available technology.

5 14–3503.

6 (a) To protect personal **INFORMATION OR PRIVATE** information from
7 unauthorized access, use, modification, or disclosure, a business that owns or licenses
8 personal **INFORMATION OR PRIVATE** information of an individual residing in the
9 State shall implement and maintain reasonable security procedures and practices that
10 are appropriate to the nature of the personal **INFORMATION OR PRIVATE** information
11 owned or licensed and the nature and size of the business and its operations.

12 (b) **(1) THIS SUBSECTION SHALL APPLY TO A WRITTEN CONTRACT**
13 **THAT IS ENTERED INTO ON OR AFTER JANUARY 1, 2014.**

14 **[(1)] (2)** A business that uses a nonaffiliated third party as a service
15 provider to perform services for the business and discloses personal **INFORMATION**
16 **OR PRIVATE** information about an individual residing in the State under a written
17 contract with the third party shall require by contract that the third party implement
18 and maintain reasonable security procedures and practices that:

19 (i) Are appropriate to the nature of the personal
20 **INFORMATION OR PRIVATE** information disclosed to the nonaffiliated third party;
21 and

22 (ii) Are reasonably designed to help protect the personal
23 **INFORMATION OR PRIVATE** information from unauthorized access, use, modification,
24 disclosure, or destruction.

25 **[(2) This subsection shall apply to a written contract that is entered**
26 **into on or after January 1, 2009.]**

27 14–3504.

28 (a) In this section:

29 (1) “Breach of the security of a system” means the unauthorized
30 acquisition of computerized data that compromises the security, confidentiality, or
31 integrity of the [personal] **PRIVATE** information maintained by a business; and

1 (2) “Breach of the security of a system” does not include the good faith
2 acquisition of [personal] **PRIVATE** information by an employee or agent of a business
3 for the purposes of the business provided that the personal information **OR PRIVATE**
4 **INFORMATION** is not used or subject to further unauthorized disclosure.

5 (3) **“IDENTITY FRAUD” MEANS ANY ACTIVITY PROHIBITED UNDER**
6 **§ 8-301(B) OR (C) OF THE CRIMINAL LAW ARTICLE.**

7 (b) (1) A business that owns or licenses computerized data that includes
8 [personal] **PRIVATE** information of an individual residing in the State, when it
9 discovers or is notified of a breach of the security of a system, shall conduct in good
10 faith a reasonable and prompt investigation to determine [the likelihood that]
11 **WHETHER THE UNAUTHORIZED ACQUISITION OF [personal] PRIVATE** information
12 of the individual has [been] **CREATED** or [will be misused as a result of the breach] **IS**
13 **REASONABLY LIKELY TO CREATE A MATERIAL RISK OF IDENTITY FRAUD.**

14 (2) If, after the investigation is concluded, the business determines
15 that [misuse] **THE UNAUTHORIZED ACQUISITION** of the individual’s [personal]
16 **PRIVATE** information has [occurred] **CREATED** or is reasonably likely to [occur as a
17 result of a breach of the security of a system,] **CREATE A MATERIAL RISK OF**
18 **IDENTITY FRAUD**, the business shall notify the 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 conducts the
22 investigation 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)
25 of 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
28 [personal] **PRIVATE** information that the business does not own or license shall notify
29 the owner or licensee of the [personal] **PRIVATE** information of a breach of the
30 security of a system if [it is likely that the breach] **THE UNAUTHORIZED**
31 **ACQUISITION OF THE INDIVIDUAL’S PRIVATE INFORMATION** has [resulted]
32 **CREATED** or [will result in the misuse of personal information of] **IS REASONABLY**
33 **LIKELY TO CREATE A MATERIAL RISK OF IDENTITY FRAUD FOR** an individual
34 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 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
2 **[personal] PRIVATE** information of a breach of the security of a system under
3 paragraph (1) of this subsection shall share with the owner or licensee information
4 relative to the breach.

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

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

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

11 (2) If notification is delayed under paragraph (1)(i) of this subsection,
12 notification shall be given as soon as reasonably practicable, **BUT NOT LATER THAN**
13 **45 DAYS** after the law enforcement agency determines that it will not impede a
14 criminal investigation and will not jeopardize homeland or national security.

15 (e) The notification required under subsections (b) and (c) of this section may
16 be given:

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

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

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

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

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

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

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

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

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

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

5 (2) Conspicuous posting of the notice on the website of the business, if
6 the business maintains a website; and

7 (3) Notification to statewide media.

8 (g) The notification required under subsection (b) of this section shall
9 include:

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

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

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

19 (4) (i) The toll-free telephone numbers, addresses, and website
20 addresses for:

21 1. The Federal Trade Commission; and

22 2. The Office of the Attorney General; and

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

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

28 (i) A waiver of any provision of this section is contrary to public policy and is
29 void and unenforceable.

30 (j) Compliance with this section does not relieve a business from a duty to
31 comply with any other requirements of federal law relating to the protection and
32 privacy of personal **INFORMATION OR PRIVATE** information.

1 14–3505.

2 The provisions of this subtitle are exclusive and shall preempt any provision of
3 local law.

4 14–3506.

5 (a) If a business is required under § 14–3504 of this subtitle to give notice of
6 a breach of the security of a system to 1,000 or more individuals, the business also
7 shall notify, [without unreasonable delay] **NOT LATER THAN 45 DAYS AFTER**
8 **NOTICE OF A BREACH IS GIVEN TO INDIVIDUALS**, each consumer reporting agency
9 that compiles and maintains files on consumers on a nationwide basis, as defined by
10 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notices.

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

14 14–3507.

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

18 (b) A business that complies with the requirements for notification
19 procedures, the protection or security of personal information, or the destruction of
20 personal **INFORMATION OR PRIVATE** information under the rules, regulations,
21 procedures, or guidelines established by the primary or functional federal or State
22 regulator of the business shall be deemed to be in compliance with this subtitle.

23 (c) (1) A business that is subject to and in compliance with § 501(b) of the
24 federal Gramm–Leach–Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and
25 Accurate Transactions Act, 15 U.S.C. § 1681W, the federal Interagency Guidelines
26 Establishing Information Security Standards, and the federal Interagency Guidance
27 on Response Programs for Unauthorized Access to Customer Information and
28 Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be
29 in compliance with this subtitle.

30 (2) An affiliate that complies with § 501(b) of the federal
31 Gramm–Leach–Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate
32 Transactions Act, 15 U.S.C. § 1681W, the federal Interagency Guidelines Establishing
33 Information Security Standards, and the federal Interagency Guidance on Response
34 Programs for Unauthorized Access to Customer Information and Customer Notice,
35 and any revisions, additions, or substitutions, shall be deemed to be in compliance
36 with this subtitle.

37 14–3508.

1 A violation of this subtitle:

2 (1) Is an unfair or deceptive trade practice within the meaning of Title
3 13 of this article; and

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

6 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
7 October 1, 2013.