HOUSE BILL 974

I3 (7lr1710)

ENROLLED BILL

— Economic Matters/Finance —

Introduced by **Delegates Carey and Lisanti**

Read and Examined by Proofreaders:

_____

Proofreader.

_____

Proofreader.

Sealed with the Great Seal and presented to the Governor, for his approval this

_____ day of _____ at _____ o'clock, _____M.

_____

Speaker.

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~~ *a* certain ~~term~~ ~~terms~~ *term*; altering certain definitions; providing
15   for a delayed effective date; and generally relating to the protection of personal

1   information contained in the records of businesses, owned or licensed by businesses,
2   or included in computerized data owned, licensed, or maintained by businesses.

3   BY repealing and reenacting, with amendments,
4   Article – Commercial Law
5   Section 14–3501, 14–3502, 14–3504, ~~and~~ ~~14–3506~~, and 14–3507
6   Annotated Code of Maryland
7   (2013 Replacement Volume and 2016 Supplement)

8   BY repealing and reenacting, without amendments,
9   Article – Commercial Law
10   Section 14–3503, 14–3505, ~~14–3507~~, *14–3506,* and 14–3508
11   Annotated Code of Maryland
12   (2013 Replacement Volume and 2016 Supplement)

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

Article – Commercial Law

16   14–3501.

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

18   (b)   (1)   "Business" means a sole proprietorship, partnership, corporation,
19   association, or any other business entity, whether or not organized to operate at a profit.

20   (2)   "Business" includes a financial institution organized, chartered,
21   licensed, or otherwise authorized under the laws of this State, any other state, the United
22   States, or any other country, and the parent or subsidiary of a financial institution.

23   (c)   "Encrypted" means the **[**transformation of data through the use of an
24   algorithmic process into a form in which there is a low probability of assigning meaning
25   without use of a confidential process or key**]** **PROTECTION OF DATA IN ELECTRONIC OR**
26   **OPTICAL FORM~~, IN STORAGE OR IN TRANSIT,~~ USING AN ENCRYPTION TECHNOLOGY**
27   **THAT~~:~~**

28   ~~(1)~~   ~~HAS   BEEN   ADOPTED   OR   APPROVED   BY   AN   ESTABLISHED~~
29   ~~STANDARDS–SETTING   BODY   OF   THE   FEDERAL   GOVERNMENT,   INCLUDING   THE~~
30   ~~FEDERAL   INFORMATION   PROCESSING   STANDARDS   ISSUED   BY   THE   NATIONAL~~
31   ~~INSTITUTE OF STANDARDS AND TECHNOLOGY; AND~~

32   ~~(2)~~   ~~RENDERS~~ *RENDERS* **THE DATA INDECIPHERABLE WITHOUT AN**
33   **ASSOCIATED CRYPTOGRAPHIC KEY NECESSARY TO ENABLE DECRYPTION OF THE**
34   **DATA.**

1   **(D)**   "H~~EALTH INFORMATION~~" ~~HAS THE MEANING STATED IN 45 C.F.R. §~~
2   ~~160.103~~ *MEANS ANY INFORMATION CREATED BY AN ENTITY COVERED BY THE*
3   *FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996*
4   *REGARDING AN INDIVIDUAL'S MEDICAL HISTORY, MEDICAL CONDITION, OR MEDICAL*
5   *TREATMENT OR DIAGNOSIS.*

6   ~~(d)~~ **(E)**   (1)   "Personal information" means ~~an~~**:**

7   *(I)*   **A**N individual's first name or first initial and last name in
8   combination with any one or more of the following data elements, when the name or the
9   data elements are not encrypted, redacted, or otherwise protected by another method that
10   renders the information unreadable or unusable:

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

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

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

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

23   ~~(v)~~   *5.*   **A HEALTH INSURANCE POLICY OR CERTIFICATE**
24   **NUMBER OR HEALTH INSURANCE SUBSCRIBER IDENTIFICATION NUMBER** ~~THAT~~**, IN**
25   **COMBINATION WITH A UNIQUE IDENTIFIER USED BY AN INSURER OR AN EMPLOYER**
26   **THAT IS SELF–INSURED,** ~~WOULD PERMIT~~ *THAT* **PERMITS ACCESS TO AN**
27   **INDIVIDUAL'S** ~~MEDICAL~~ **HEALTH INFORMATION;** *OR*

28   ~~(VI)~~   ~~A USER NAME OR E–MAIL ADDRESS THAT, IN COMBINATION~~
29   ~~WITH A PASSWORD OR SECURITY QUESTION AND ANSWER, WOULD PERMIT PERMITS~~
30   ~~ACCESS TO AN INDIVIDUAL'S ONLINE E–MAIL ACCOUNT OR FINANCIAL ACCOUNT; OR~~

31   ~~(VII)~~ *6.*   ~~ANY BIOMETRIC~~ **BIOMETRIC DATA OF AN**
32   **INDIVIDUAL,** ~~INCLUDING~~ ~~DATA~~ **GENERATED BY AUTOMATIC MEASUREMENTS OF AN**
33   **INDIVIDUAL'S BIOLOGICAL CHARACTERISTICS SUCH AS A FINGERPRINT, VOICE**
34   **PRINT, GENETIC PRINT,** ~~OR~~ **RETINA OR IRIS IMAGE, OR OTHER UNIQUE BIOLOGICAL**
35   **CHARACTERISTIC, THAT CAN BE USED TO** ~~IDENTIFY THE INDIVIDUAL~~ **UNIQUELY**

1   AUTHENTICATE THE INDIVIDUAL'S IDENTITY WHEN THE INDIVIDUAL ACCESSES A
2   SYSTEM OR ACCOUNT; *OR*

3   *(II)   A USER NAME OR E–MAIL ADDRESS IN COMBINATION WITH A*
4   *PASSWORD OR SECURITY QUESTION AND ANSWER THAT PERMITS ACCESS TO AN*
5   *INDIVIDUAL'S E–MAIL ACCOUNT.*

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

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

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

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

13   ~~(E)~~ (F)   ~~"REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS~~
14   ~~DATA SECURITY PROCEDURES AND PRACTICES THAT:~~

15   ~~(1)   ARE DEVELOPED IN GOOD FAITH; AND SET~~

16   ~~(2)   ARE SET FORTH IN A WRITTEN INFORMATION SECURITY POLICY;~~
17   ~~THAT CLEARLY DEMONSTRATES THAT THE PROCEDURES AND PRACTICES:~~

18   ~~(1)~~ (3)   ~~COORDINATE~~ DESIGNATE ONE OR MORE EMPLOYEES OR
19   ~~CONTRACTORS TO COORDINATE AN INFORMATION SECURITY PROGRAM;~~

20   ~~(2)~~ (4)   ~~REQUIRE A RISK ASSESSMENT TO IDENTIFY REASONABLY~~
21   ~~FORESEEABLE   INTERNAL   AND   EXTERNAL   RISKS   TO   THE   SECURITY,~~
22   ~~CONFIDENTIALITY, AND INTEGRITY OF PERSONAL INFORMATION AND TO ASSESS~~
23   ~~THE   SUFFICIENCY   OF   ANY   EXISTING   SAFEGUARDS   IN   PLACE   TO   CONTROL   THE~~
24   ~~IDENTIFIED RISKS;~~

25   ~~(3)~~ (5)   ~~ONCE   A   RISK   ASSESSMENT   IS   COMPLETED,   INCLUDE~~
26   ~~DESIGN   SAFEGUARDS   TO   CONTROL   ADDRESS   THE   IDENTIFIED   RISKS   AND   TO~~
27   ~~REGULARLY MONITOR THE EFFECTIVENESS OF THE CONTROLS;~~

28   ~~(4)~~ (6)   ~~ENSURE,   IN   ANY   CONTRACT   WITH   A   SERVICE   PROVIDER~~
29   ~~ENTERED INTO ON OR AFTER JANUARY 1, 2018, THAT THE SERVICE PROVIDER IS~~
30   ~~CAPABLE   OF   PROVIDING   APPROPRIATE   SAFEGUARDS   FOR   THE   PERSONAL~~
31   ~~INFORMATION; AND~~

1 ~~(5) (7)~~   ~~EVALUATE AND ADJUST THE INFORMATION SECURITY~~
2 ~~PROGRAM PERIODICALLY~~ ~~BASED ON:~~

3   ~~(I)~~   ~~THE FINDINGS OF THE REGULAR MONITORING AND~~
4 ~~TESTING OF INFORMATION SAFEGUARDS;~~

5   ~~(II)~~   ~~MATERIAL CHANGES TO OPERATIONS OR BUSINESS~~
6 ~~ARRANGEMENTS; OR~~

7   ~~(III) (II)~~   ~~CIRCUMSTANCES~~ ~~NEW CIRCUMSTANCES~~ ~~THAT THE~~
8 ~~BUSINESS KNOWS OR HAS REASON TO KNOW~~ ~~SHOULD KNOW~~ ~~MAY HAVE A MATERIAL~~
9 ~~IMPACT ON THE INFORMATION SECURITY PROGRAM OF THE BUSINESS.~~

10 **[**(e)**]** ~~(F)~~ ~~(G)~~ *(F)*   "Records" means information that is inscribed on a tangible
11 medium or that is stored in an electronic or other medium and is retrievable in perceivable
12 form.

13 14–3502.

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

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

21   (1)   The sensitivity of the records;

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

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

24   (4)   Available technology.

25 14–3503.

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

31   (b)   (1)   A business that uses a nonaffiliated third party as a service provider to
32 perform services for the business and discloses personal information about an individual

1 residing in the State under a written contract with the third party shall require by contract
2 that the third party implement and maintain reasonable security procedures and practices
3 that:

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

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

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

10 14–3504.

11   (a)   In this section:

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

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

19   (b)   (1)   A business that owns or licenses computerized data that includes
20 personal information of an individual residing in the State, when it discovers or is notified
21 of a breach of the security of a system, shall conduct in good faith a reasonable and prompt
22 investigation to determine **[**the likelihood that**]** ~~WHETHER THERE IS A REASONABLE~~
23 ~~LIKELIHOOD THAT AN UNAUTHORIZED ACCESSING OR ACQUISITION OF THE~~ personal
24 information of the individual has **[**been or will be misused ~~OCCURRED OR WILL OCCUR~~
25 *BEEN OR WILL BE MISUSED* as a result of the breach**]** ~~OCCURRED~~.

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

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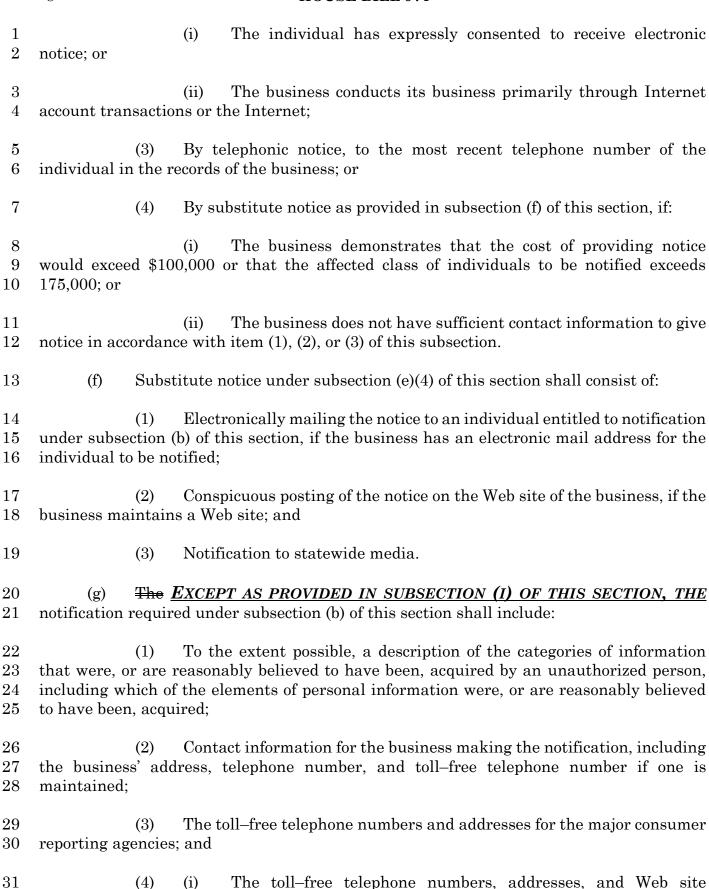35 **CONCLUDES** the investigation required under paragraph (1) of this subsection.

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

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

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

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

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

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

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

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

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

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

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

1   (i)   The individual has expressly consented to receive electronic
2   notice; or

3   (ii)   The business conducts its business primarily through Internet
4   account transactions or the Internet;

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

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

8   (i)   The business demonstrates that the cost of providing notice
9   would exceed $100,000 or that the affected class of individuals to be notified exceeds
10   175,000; or

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

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

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

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

19   (3)   Notification to statewide media.

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

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

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

29   (3)   The toll–free telephone numbers and addresses for the major consumer
30   reporting agencies; and

31   (4)   (i)   The toll–free telephone numbers, addresses, and Web site
32   addresses for:

1   1.   The Federal Trade Commission; and

2   2.   The Office of the Attorney General; and

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

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

8   *(I)   (1)   IN THE CASE OF A BREACH OF THE SECURITY OF A SYSTEM*
9 *INVOLVING PERSONAL INFORMATION THAT PERMITS ACCESS TO AN INDIVIDUAL'S*
10 *E–MAIL ACCOUNT UNDER § 14–3501(E)(1)(II) OF THIS SUBTITLE AND NO OTHER*
11 *PERSONAL INFORMATION UNDER § 14–3501(E)(1)(I) OF THIS SUBTITLE, THE*
12 *BUSINESS MAY COMPLY WITH THE NOTIFICATION REQUIREMENT UNDER*
13 *SUBSECTION (B) OF THIS SECTION BY PROVIDING THE NOTIFICATION IN*
14 *ELECTRONIC OR OTHER FORM THAT DIRECTS THE INDIVIDUAL WHOSE PERSONAL*
15 *INFORMATION HAS BEEN BREACHED PROMPTLY TO:*

16   *(I)   CHANGE THE INDIVIDUAL'S PASSWORD AND SECURITY*
17 *QUESTION OR ANSWER, AS APPLICABLE; OR*

18   *(II)   TAKE OTHER STEPS APPROPRIATE TO PROTECT THE E– MAIL*
19 *ACCOUNT WITH THE BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE*
20 *INDIVIDUAL USES THE SAME USER NAME OR E–MAIL AND PASSWORD OR SECURITY*
21 *QUESTION OR ANSWER.*

22   *(2)   SUBJECT TO PARAGRAPH (3) OF THIS SUBSECTION, THE*
23 *NOTIFICATION PROVIDED UNDER PARAGRAPH (1) OF THIS SUBSECTION MAY BE*
24 *GIVEN TO THE INDIVIDUAL BY ANY METHOD DESCRIBED IN THIS SECTION.*

25   *(3)   (I)   EXCEPT AS PROVIDED IN SUBPARAGRAPH (II) OF THIS*
26 *PARAGRAPH, THE NOTIFICATION PROVIDED UNDER PARAGRAPH (1) OF THIS*
27 *SUBSECTION MAY NOT BE GIVEN TO THE INDIVIDUAL BY SENDING NOTIFICATION BY*
28 *E–MAIL TO THE E–MAIL ACCOUNT AFFECTED BY THE BREACH.*

29   *(II)   THE NOTIFICATION PROVIDED UNDER PARAGRAPH (1) OF*
30 *THIS SUBSECTION MAY BE GIVEN BY A CLEAR AND CONSPICUOUS NOTICE DELIVERED*
31 *TO THE INDIVIDUAL ONLINE WHILE THE INDIVIDUAL IS CONNECTED TO THE*
32 *AFFECTED E–MAIL ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR ONLINE*
33 *LOCATION FROM WHICH THE BUSINESS KNOWS THE INDIVIDUAL CUSTOMARILY*
34 *ACCESSES THE ACCOUNT.*

1   ~~(i)~~ *(J)*   A waiver of any provision of this section is contrary to public policy and
2   is void and unenforceable.

3   ~~(j)~~ *(K)*   Compliance with this section does not relieve a business from a duty to
4   comply with any other requirements of federal law relating to the protection and privacy of
5   personal information.

6   14–3505.

7   The provisions of this subtitle are exclusive and shall preempt any provision of local
8   law.

9   14–3506.

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

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

18 14–3507.

19   (a)   In this section, "affiliate" means a company that controls, is controlled by, or
20 is under common control with a business described in subsection (c)(1) **OR (D)(1)** of this
21 section.

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

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

34   (2)   An   affiliate   that   complies   with   §   501(b)   of   the   federal
35 Gramm–Leach–Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit

1 Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines Establishing
2 Information Security Standards, and the federal Interagency Guidance on Response
3 Programs for Unauthorized Access to Customer Information and Customer Notice, and any
4 revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle.

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

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

11 14–3508.

12   A violation of this subtitle:

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

15   (2)   Is subject to the enforcement and penalty provisions contained in Title
16 13 of this article.

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

Approved:

_____
                                       Governor.

_____
                    Speaker of the House of Delegates.

_____
                     President of the Senate.