HOUSE BILL 974

I3 7lr1710
CF SB 525

By: **Delegates Carey and Lisanti**
Introduced and read first time: February 6, 2017
Assigned to: Economic Matters

A BILL ENTITLED

AN ACT concerning

Maryland Personal Information Protection Act – Revisions

FOR the purpose of requiring a certain business, when destroying an employee's or a former employee's records that contain certain personal information of the employee or former employee, to take certain steps to protect against unauthorized access to or use of the information; altering the circumstances under which a certain business that owns, licenses, or maintains computerized data that includes certain personal information of an individual residing in the State must conduct a certain investigation and notify certain persons of a breach of the security of a system; specifying the time at which certain notice must be given; defining a certain term; altering certain definitions; and generally relating to the protection of personal information contained in the records of businesses, owned or licensed by businesses, or included in computerized data owned, licensed, or maintained by businesses.

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

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

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

Article – Commercial Law

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

14–3501.

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

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

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

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

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

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

(d) (1) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

(i) A Social Security number**, AN INDIVIDUAL TAXPAYER IDENTIFICATION NUMBER, A PASSPORT NUMBER, OR OTHER IDENTIFICATION NUMBER ISSUED BY THE FEDERAL GOVERNMENT**;

(ii) A driver's license number **OR STATE IDENTIFICATION CARD NUMBER**;

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

(iv) **[**An Individual Taxpayer Identification Number**]** **MEDICAL INFORMATION, INCLUDING INFORMATION ABOUT AN INDIVIDUAL'S MENTAL HEALTH;**

(V) A HEALTH INSURANCE POLICY NUMBER OR HEALTH INSURANCE SUBSCRIBER IDENTIFICATION NUMBER THAT, IN COMBINATION WITH A UNIQUE IDENTIFIER USED BY AN INSURER, WOULD PERMIT ACCESS TO AN INDIVIDUAL'S MEDICAL INFORMATION;

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

(VII) ANY BIOMETRIC DATA OF AN INDIVIDUAL, INCLUDING A FINGERPRINT, VOICE PRINT, GENETIC PRINT, OR RETINA OR IRIS IMAGE, THAT CAN BE USED TO IDENTIFY THE INDIVIDUAL.

(2) "Personal information" does not include:

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

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

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

(E) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS DATA SECURITY PROCEDURES AND PRACTICES DEVELOPED IN GOOD FAITH AND SET FORTH IN A WRITTEN INFORMATION SECURITY POLICY THAT CLEARLY DEMONSTRATES THAT THE PROCEDURES AND PRACTICES:

(1) COORDINATE AN INFORMATION SECURITY PROGRAM;

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

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

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

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

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

(II) MATERIAL CHANGES TO OPERATIONS OR BUSINESS ARRANGEMENTS; OR

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

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

14–3502.

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

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

(1) The sensitivity of the records;

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

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

(4) Available technology.

14–3503.

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

(b) (1) A business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about an individual residing in the State under a written contract with the third party shall require by contract

that the third party implement and maintain reasonable security procedures and practices that:

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

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

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

14–3504.

(a) In this section:

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

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

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

(2) If, after the investigation is concluded, the business determines that **[**misuse**]** **AN UNAUTHORIZED ACCESSING OR ACQUISITION** of the individual's personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach.

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

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

(c) (1) A business that maintains computerized data that includes personal information that the business does not own or license shall notify the owner or licensee of the personal information of a breach of the security of a system if it is likely that the breach has resulted or will result in the **[**misuse**]** **ACCESSING OR ACQUISITION** of personal information of an individual residing in the State.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) Notification to statewide media.

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

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

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

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

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

1. The Federal Trade Commission; and

2. The Office of the Attorney General; and

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

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

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

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

14–3505.

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

14–3506.

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

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

14–3507.

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

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

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

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

14–3508.

A violation of this subtitle:

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

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

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