SENATE BILL 217

I3 1lr0903
(PRE–FILED) CF HB 117

By: **Senator Sydnor**
Requested: October 9, 2020
Introduced and read first time: January 13, 2021
Assigned to: Finance

A BILL ENTITLED

AN ACT concerning

Maryland Personal Information Protection Act – Revisions

FOR the purpose of altering the circumstances under which an owner or licensee of computerized data is required to notify a certain individual of a breach of the security of a system; altering the time period within which a business is required to provide a certain notification relating to a breach of the security of a system; requiring a business, credit card processor, and vendor to take reasonable care to protect against unauthorized access to personal information connected to credit and debit cards in accordance with certain provisions of law; establishing that a business, credit card processor, or vendor is liable to a certain financial institution for certain reimbursement under certain circumstances; providing that a business, credit card processor, or vendor is not liable to a certain financial institution for a certain breach under certain circumstances; requiring a trier of fact in a certain action to make a certain determination; authorizing a certain trier of fact in a certain action to reduce certain damages under certain circumstances; authorizing a court to award reasonable attorney's fees and costs to a prevailing party in a certain action; providing for the construction of this Act; defining certain terms; making conforming changes; and generally relating to the Maryland Personal Information Protection Act.

BY repealing and reenacting, with amendments,
Article – Commercial Law
Section 14–3501 and 14–3504
Annotated Code of Maryland
(2013 Replacement Volume and 2020 Supplement)

BY adding to
Article – Commercial Law
Section 14–3504.1
Annotated Code of Maryland

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

(2013 Replacement Volume and 2020 Supplement)

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

Article – Commercial Law

14–3501.

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

(B) (1) "BREACH OF THE SECURITY OF A SYSTEM" MEANS THE UNAUTHORIZED ACQUISITION OF COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF THE PERSONAL INFORMATION MAINTAINED BY A BUSINESS.

(2) "BREACH OF THE SECURITY OF A SYSTEM" DOES NOT INCLUDE THE GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A BUSINESS FOR THE PURPOSES OF THE BUSINESS, IF THE PERSONAL INFORMATION IS NOT USED OR SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

[(b)**] (C)** (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)**] (D)** "Encrypted" means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.

[(d)**] (E)** "Health information" means any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 regarding an individual's medical history, medical condition, or medical treatment or diagnosis.

[(e)**] (F)** (1) "Personal information" means:

(i) 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:

1. A Social Security number, an Individual Taxpayer

Identification Number, a passport number, or other identification number issued by the federal government;

2. A driver's license number or State identification card number;

3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;

4. Health information, including information about an individual's mental health;

5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self–insured, that permits access to an individual's health information; or

6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or

(ii) A user name or e–mail address in combination with a password or security question and answer that permits access to an individual's e–mail account.

(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.

[(f)**] (G)** "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.

14–3504.

[(a) In this section:

(1) "Breach of the security of a system" means the unauthorized 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 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)**] (A)** (1) A business that owns, licenses, or maintains computerized data that includes personal information of an individual residing in the State, when it discovers or is notified that it incurred a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.

(2) Subject to subsection **[**(c)(4)**] (B)(4)** of this section, **[**if,**]** after the investigation is concluded, **THE OWNER OR LICENSEE OF THE COMPUTERIZED DATA SHALL NOTIFY THE INDIVIDUAL OF THE BREACH UNLESS** the business **REASONABLY** determines that the breach of the security of the system **[**creates**] DOES NOT CREATE** a likelihood that personal information has been or will be misused**[**, the owner or licensee of the computerized data shall notify the individual of the breach**]**.

(3) Except as provided in subsection **[**(d)**] (C)** of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable, but not later than 45 days after the business **[**concludes the investigation required under paragraph (1) of this subsection**] DISCOVERS OR IS NOTIFIED OF THE BREACH**.

(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)**] (B)** (1) A business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license, when it discovers or is notified of a breach of the security of a system, shall notify, as soon as practicable, the owner or licensee of the personal information of the breach of the security of a system.

(2) Except as provided in subsection **[**(d)**] (C)** of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable, but not later than 45 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.

(4) (i) If the business that incurred the breach of the security of a system is not the owner or licensee of the computerized data, the business may not charge the owner or licensee of the computerized data a fee for providing information that the owner or licensee needs to make a notification under subsection **[**(b)(2)**]** **(A)(2)** of this section.

(ii) The owner or licensee of the computerized data may not use information relative to the breach of the security of a system for purposes other than:

1. Providing notification of the breach;

2. Protecting or securing personal information; or

3. Providing notification to national information security organizations created for information–sharing and analysis of security threats, to alert and avert new or expanded breaches.

[(d)**]** **(C)** (1) The notification required under subsections **[**(b) and (c)**]** **(A) AND (B)** 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)**]** **(D)** The notification required under subsection **[**(b)**]** **(A)** 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)**] (E)** 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)**] (E)** Substitute notice under subsection **[**(e)(4)**] (D)(4)** of this section shall consist of:

(1) Electronically mailing the notice to an individual entitled to notification under subsection **[**(b)**] (A)** 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 website of the business, if the business maintains a website; and

(3) Notification to statewide media.

[(g)**] (F)** Except as provided in subsection **[**(i)**] (H)** of this section, the notification required under subsection **[**(b)**] (A)** 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 website 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)**] (G)** Prior to giving the notification required under subsection **[**(b)**] (A)** of this section and subject to subsection **[**(d)**] (C)** 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)**] (H)** (1) In the case of a breach of the security of a system involving personal information that permits access to an individual's e–mail account under § **[**14–3501(e)(1)(ii)**] 14–3501(F)(1)(II)** of this subtitle and no other personal information under § **[**14–3501(e)(1)(i)**] 14–3501(F)(1)(I)** of this subtitle, the business may comply with the notification requirement under subsection **[**(b)**] (A)** of this section by providing the notification in electronic or other form that directs the individual whose personal information has been breached promptly to:

(i) Change the individual's password and security question or answer, as applicable; or

(ii) Take other steps appropriate to protect the e–mail account with the business and all other online accounts for which the individual uses the same user name or e–mail and password or security question or answer.

(2) Subject to paragraph (3) of this subsection, the notification provided under paragraph (1) of this subsection may be given to the individual by any method described in this section.

(3) (i) Except as provided in subparagraph (ii) of this paragraph, the notification provided under paragraph (1) of this subsection may not be given to the individual by sending notification by e–mail to the e–mail account affected by the breach.

(ii) The notification provided under paragraph (1) of this subsection may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected e–mail account from an Internet Protocol address or online location from which the business knows the individual customarily accesses the account.

[(j)**] (I)** A waiver of any provision of this section is contrary to public policy and is void and unenforceable.

[(k)**] (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.

14–3504.1.

(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(2) "CERTIFIED COMPLIANT" MEANS A BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR WHOSE SECURITY ASSESSMENT OF COMPLIANCE WAS VALIDATED BY THE PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL'S ANNUAL SECURITY ASSESSMENT NO MORE THAN 1 YEAR BEFORE THE TIME OF A BREACH OF THE SECURITY OF A SYSTEM.

(3) "CREDIT CARD PROCESSOR" HAS THE MEANING STATED IN § 12–1401 OF THIS ARTICLE.

(4) "DE FACTO COMPLIANT" MEANS A BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR WHOSE SECURITY PROCEDURES WERE COMPLIANT WITH THE PAYMENT CARD INDUSTRY SECURITY STANDARDS OR A SUBSTANTIALLY SIMILAR STANDARD AT THE TIME OF THE BREACH OF THE SECURITY OF A SYSTEM, BUT WHO LACKS A FORMAL CERTIFICATION OF COMPLIANCE.

(5) "VENDOR" MEANS A PERSON THAT MANUFACTURES AND SELLS SOFTWARE OR EQUIPMENT THAT IS DESIGNED TO PROCESS, TRANSMIT, OR STORE PERSONAL INFORMATION OR THAT MAINTAINS PERSONAL INFORMATION THAT IT DOES NOT OWN.

(B) A BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR SHALL TAKE REASONABLE CARE TO PROTECT AGAINST UNAUTHORIZED ACCESS TO PERSONAL INFORMATION CONNECTED TO A CREDIT OR DEBIT CARD IN ACCORDANCE WITH § 14–3503 OF THIS SUBTITLE.

(C) (1) (I) A BUSINESS OR CREDIT CARD PROCESSOR THAT FAILS TO COMPLY WITH SUBSECTION (B) OF THIS SECTION IS LIABLE TO THE FINANCIAL INSTITUTION THAT ISSUED THE CREDIT OR DEBIT CARD FOR REIMBURSEMENT OF THE ACTUAL AND REASONABLE COSTS RELATED TO THE REISSUANCE OF A CREDIT OR DEBIT CARD IF THE FAILURE IS FOUND TO BE THE PROXIMATE CAUSE OF A BREACH OF THE SECURITY OF A SYSTEM.

(II) A FINANCIAL INSTITUTION IS NOT REQUIRED TO SHOW PHYSICAL INJURY SUFFERED IN CONNECTION WITH A BREACH OF THE SECURITY OF A SYSTEM TO RECOVER UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH.

(2) A VENDOR THAT FAILS TO COMPLY WITH SUBSECTION (B) OF THIS SECTION IS LIABLE TO THE FINANCIAL INSTITUTION THAT ISSUED THE CREDIT OR DEBIT CARD FOR REIMBURSEMENT OF THE ACTUAL AND REASONABLE COSTS RELATED TO THE REISSUANCE OF A CREDIT OR DEBIT CARD IF THE:

(I) DAMAGES INCURRED WERE PROXIMATELY CAUSED BY THE

NEGLIGENCE OF THE VENDOR; AND

(II) CLAIM IS NOT LIMITED BY ANOTHER PROVISION OF LAW OR A CONTRACT TO WHICH THE FINANCIAL INSTITUTION IS A PARTY.

(D) (1) FOR THE PURPOSES OF THIS SUBSECTION, A BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR'S SECURITY ASSESSMENT OF COMPLIANCE IS IRREVOCABLE.

(2) A BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR IS NOT LIABLE UNDER THIS SECTION IF:

(I) THE PERSONAL INFORMATION WAS ENCRYPTED AT THE TIME OF THE BREACH OF THE SECURITY OF A SYSTEM; AND

(II) THE BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR WAS CERTIFIED COMPLIANT, OR CAN SHOW EVIDENCE THAT IT WAS DE FACTO COMPLIANT, AT THE TIME OF THE BREACH OF THE SECURITY OF A SYSTEM.

(E) (1) (I) IN AN ACTION BROUGHT UNDER THIS SECTION, THE TRIER OF FACT SHALL DETERMINE THE PERCENTAGE OF THE TOTAL FAULT THAT IS ATTRIBUTABLE TO EACH ENTITY THAT WAS THE PROXIMATE CAUSE OF THE CLAIMANT'S DAMAGES.

(II) A TRIER OF FACT MAY REDUCE DAMAGES AWARDED TO A FINANCIAL INSTITUTION BY ANY AMOUNT THE FINANCIAL INSTITUTION RECOVERS FROM A CREDIT CARD COMPANY IN CONNECTION WITH THE BREACH OF THE SECURITY OF A SYSTEM FOR COSTS ASSOCIATED WITH CREDIT OR DEBIT CARD REISSUANCE.

(2) IN AN ACTION BROUGHT UNDER THIS SECTION, THE COURT MAY AWARD REASONABLE ATTORNEY'S FEES AND COSTS TO THE PREVAILING PARTY.

(F) THIS SECTION MAY NOT BE CONSTRUED TO PREVENT:

(1) AN ENTITY RESPONSIBLE FOR HANDLING PERSONAL INFORMATION ON BEHALF OF A BUSINESS OR CREDIT CARD PROCESSOR FROM BEING MADE A PARTY TO AN ACTION UNDER THIS SECTION; OR

(2) A BUSINESS, CREDIT CARD PROCESSOR, OR VENDOR FROM ASSERTING ANY DEFENSE OTHERWISE AVAILABLE IN AN ACTION.

(G) THE RIGHTS, REMEDIES, AND PROHIBITIONS PROVIDED UNDER THIS

SECTION ARE IN ADDITION TO AND CUMULATIVE OF ANY OTHER RIGHT, REMEDY, OR PROHIBITION PROVIDED BY LAW.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2021.