HOUSE BILL 1154

I3 9lr0810
CF SB 693

By: **Delegates Howard, Buckel, Chisholm, Malone, and Saab**
Introduced and read first time: February 8, 2019
Assigned to: Economic Matters

Committee Report: Favorable with amendments
House action: Adopted
Read second time: March 13, 2019

CHAPTER _____

AN ACT concerning

Maryland Personal Information Protection Act – Security Breach Notification Requirements – Modifications

FOR the purpose of altering the applicability of certain security breach investigation requirements to certain businesses; altering the applicability of certain security breach notification requirements to a certain owner or licensee of computerized data; prohibiting a certain business from charging a certain owner or licensee of computerized data a fee for providing information that the owner or licensee needs to provide a certain notification; prohibiting a certain owner or licensee from using certain information for certain purposes; and generally relating to the Maryland Personal Information Protection Act.

BY repealing and reenacting, with amendments,
Article – Commercial Law
Section 14–3504
Annotated Code of Maryland
(2013 Replacement Volume and 2018 Supplement)

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

Article – Commercial Law

14–3504.

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.

(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) (1) A business that owns **[**or**],** licenses**, OR MAINTAINS** computerized data that includes personal information of an individual residing in the State, when it discovers or is notified **[**of**] 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) **[**If**] SUBJECT TO SUBSECTION (C)(4) OF THIS SECTION, IF**, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the **[**business**] OWNER OR LICENSEE OF THE COMPUTERIZED DATA** 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 45 days after the business 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 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) 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) 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 ~~PROVIDING~~:

1. PROVIDING NOTIFICATION OF THE BREACH ~~OR PROTECTING~~;

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) (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 subsection (b) 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**]** **WEBSITE** of the business, if the business maintains a **[**Web site**]** **WEBSITE**; and

(3) Notification to statewide media.

(g) Except as provided in subsection (i) of this section, 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**]** **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) 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) (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) of this subtitle and no other personal information under § 14–3501(e)(1)(i) of this subtitle, the business may comply with the notification requirement under subsection (b) 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) A waiver of any provision of this section is contrary to public policy and is void and unenforceable.

(k) 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.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2019.

Approved:

_____

Governor.

_____

Speaker of the House of Delegates.

_____

President of the Senate.