

BRIAN E. FROSH
Attorney General

WILLIAM D. GRUHN
Chief

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General



STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

October 3, 2018

Honorable Gary Gensler, Chair
Financial Consumer Protection Commission
3E Senate Office Building
Annapolis, MD 21401

Re: Consumer Protection Division's Recommendations for Amendments to the
Personal Information Protection Act

Dear Mr. Gensler,

During the Commission's September 12, 2018 session, the Consumer Protection Division of the Office of the Attorney General (the "Division") provided testimony and committed to providing you with proposed amendments to the Personal Information Protection Act, Md. Code Ann., Com. Law § 13-3401, *et seq.* (2013 Repl. Vol. and 2017 Supp.) ("PIPA"). In this letter we outline our proposed amendments to PIPA. Attached, you will also find a draft of PIPA that includes our recommended additions in bold capital letters and our recommended deletions in brackets.

First, we propose expanding the scope of personal information protected by PIPA to adequately capture additional sensitive and private information being harvested from consumers for profit. In order to protect activity-tracking data collected by wearable devices, we propose adding a new paragraph (7) to Md. Code Ann., Com. Law § 14-3501(e)(1)(i), which would read: "activity-tracking data, including all data collected through an application or electronic device capable of tracking individual activity, behavior, or location; and any information or data derived therefrom." In order to protect genetic information, we propose adding a new paragraph (iii) to Md. Code Ann., Com. Law § 14-3501(e)(1), which would read: "genetic information with respect to an individual, including an individual's genetic sample; an individual's genetic tests; the genetic tests of family members of the individual; the manifestation of a disease or disorder in family members of such individual; any request for, or receipt of, a genetic test, genetic counseling, or genetic education; and any information or data derived therefrom.¹ We would recommend defining "genetic test" as "an analysis of human DNA, RNA, chromosomes,

¹ We recommend that genetic information be added as Md. Code Ann., Com. Law § 14-3501(e)(1)(iii), as opposed to a subparagraph of Md. Code Ann., Com. Law § 14-3501(e)(1)(i) because subparagraphs of (e)(1)(i) require the data to be paired with an "individual's first name or first initial and last name." Genetic information cannot be deidentified, and therefore a name need not be tied to it.

proteins, or metabolites.” We also recommend protection for one other type of personal information that we did not mention in our September 12th testimony: non-public personal information collected on social media. After the September 12th session, Facebook announced a breach that allowed access to the accounts of up to 90 million of its users, which highlighted the need for this proposed amendment. Thus, we would recommend adding a new paragraph (iv) to Md. Code Ann., Com. Law § 14-3501(e)(1), which would read: “non-public social media information about an individual, including communications, postings, pictures, videos, connections between individuals, connections between accounts, and actions.”²

Second, we would recommend a clarification that the requirement to protect personal information through the use of reasonable security procedures and practices applies to those who maintain personal information. While this duty already exists under the current law, it may help to clarify that obligation by adding “maintains” to Md. Code Ann., Com. Law § 14-3503(a).

Third, we recommend deleting the word “computerized” in Md. Code Ann., Com Law § 14-3504(a)(1). This fixes a loophole. It will clarify that hard-copy breaches trigger breach notification obligations.

Fourth, we recommend tightening the timelines for providing notice of a breach to consumers and to the Attorney General. To accomplish this, we recommend amending Md. Code Ann., Com Law § 14-3504(b)(3) to require a business to notify consumers “not later than 10 days after the business discovers or is notified of the breach of the security of a system.”³ We recommend amending Md. Code Ann., Com Law § 14-3504(c)(2) to require that a third party maintainer of personal information notify the business that owns the information “as soon as reasonably practicable, but not later than 3 days after the business discovers or is notified of the breach of the security of a system.” We also recommend changes to the provisions that allow for delays in the notification process. Currently, Md. Code Ann., Com Law § 14-3504(d) permits both a business to delay notifying consumers that it was breached, and a third-party to delay notifying the owner of the personal information that it was subject to a breach. Section 14-3504(d) permits such delays if (1) law enforcement determines that the notification will impede an investigation, or (2) to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system. We recommend only allowing the delays described in section 14-3504(d) to delay reporting to consumers, not to allow a third party to delay reporting a breach to the business that owns the personal information. We are aware of no situation where either concern would justify keeping the fact of a breach unknown to the business which owns the data. We would also recommend removing from § 14-3504(d)(1)(ii) permission to delay in order to “determine the scope of the breach of the security of a system,”

² We recommend that non-public social media information be added as Md. Code Ann., Com. Law § 14-3501(e)(1)(iv), as opposed to a subparagraph of Md. Code Ann., Com. Law § 14-3501(e)(1)(i) because subparagraphs of (e)(1)(i) require the data to be paired with an “individual’s first name or first initial and last name.” By its nature, such social media information is identifiable to an individual, and therefore a name need not be tied to it.

³ This proposal recommends requiring notice of a breach within 10 days of discovery. However, if the Commission is inclined to propose a shorter timeline, there is support for requiring notice within 72 hours of discovery. The European Union’s General Data Breach Protection Regulation (“GDPR”) (Article 33) and the New York Department of Financial Services Cybersecurity Regulations (N.Y. Comp. Codes R. & Regs. Tit. 23 § 500.17) each require notice within 72 hours of the discovery of a breach. Companies with an international reach into the EU will already be providing notice of breaches within 72 hours.

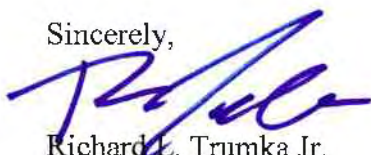
and to “identify the individuals affected.” Finalizing these determinations do not justify delay. And we recommend reducing the timeline in which to provide consumer notice after law enforcement notifies a business that notifying consumers will not impede an investigation by shortening the timeline in § 14-3504(d)(2) to 1 day.

Fifth, we recommend removing a business’s option to either provide direct notice or substitute notice, and instead require both direct and substitute notice. We recommend accomplishing this by amending Md. Code Ann., Com Law §14-3504(e) and (f) to require businesses to provide both types of notice.

Sixth, we propose adding a requirement that specific information be included in the notice that businesses provide to the Attorney General’s Office pursuant to Md. Code Ann., Com Law §14-3504(h). We recommend adding a paragraph (1) to Md. Code Ann., Com Law §14-3504(h), which would read: “The notice required by this subsection shall at least include: (i) the number of affected individuals residing in the state;⁴ (ii) a description of the breach of the security of a system, including how it occurred and any vulnerabilities that were exploited;⁵ (iii) any steps the business has taken or plans to take relating to the breach of the security of a system;⁶ and (iv) a sample of each form notice that will be sent to consumers pursuant to subsections (e) and (f).”^{7, 8}

Thank you for your consideration. Please let us know if you have any questions, or would like any further explanation of our recommendations.

Sincerely,



Richard L. Trumka Jr.
Assistant Attorney General
Office of the Maryland Attorney General

cc: Members of the Commission

⁴ Such a requirement exists in multiple states. *See, e.g.*, Ala. Code, § 8-38-6(b)(2) (Alabama); Fla. Stat. § 501,171(3)(b)(2) (Florida); Mont. Code Ann. § 30-14-1704(8) (Montana); N.H. Rev. Stat. Ann. § 359-C:20(I)(b) (New Hampshire); N.C. Gen. Stat. § 75-65(e1) (North Carolina); R.I. Gen. Laws § 11-49.3-4(a)(2) (Rhode Island); Vt. Stat. Ann. tit. 9 § 2435(b)(3)(C)(i) (Vermont); and Wash. Rev. Code § 19.255.010(15) (Washington).

⁵ Such a requirement exists in multiple states. *See, e.g.*, Ala. Code, § 8-38-6(b)(1) (Alabama); Fla. Stat. § 501,171(3)(b)(1) (Florida); N.H. Rev. Stat. Ann. § 359-C:20(IV) (New Hampshire); N.C. Gen. Stat. § 75-65(e1) (North Carolina); and Vt. Stat. Ann. tit. 9 § 2435(b)(3)(B)(i) (Vermont).

⁶ Such a requirement exists in multiple states. *See, e.g.*, Fla. Stat. § 501,171(3)(b)(3) (Florida); and N.C. Gen. Stat. § 75-65(e1) (North Carolina).

⁷ Such a requirement exists in multiple states. *See, e.g.*, Cal. Civ. Code § 1798.82(f) (California); Fla. Stat. § 501,171(3)(b)(4) (Florida); Mont. Code Ann. § 30-14-1704(8) (Montana); N.C. Gen. Stat. § 75-65(e1) (North Carolina); Or. Rev. Stat. § 646A.604(10) (Oregon); R.I. Gen. Laws § 11-49.3-4(a)(2) (Rhode Island); Va. Code Ann. § 18.2-186.6(E) (Virginia); Vt. Stat. Ann. tit. 9 § 2435(b)(3)(C)(i) (Vermont); and Wash. Rev. Code § 19.255.010(15) (Washington).

⁸ During our September 12, 2018 testimony, we also suggested that we could provide a form letter to use in notifying the Office of the Attorney General of a breach. We do not seek a legislative change related to that suggestion. Any form letter would be made available on our website.

Maryland Personal Information Protection Act

§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 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) “GENETIC TEST” MEANS AN ANALYSIS OF HUMAN DNA, RNA, CHROMOSOMES, PROTEINS, OR METABOLITES.

([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]

7. ACTIVITY-TRACKING DATA, INCLUDING ALL DATA COLLECTED THROUGH AN APPLICATION OR ELECTRONIC DEVICE CAPABLE OF TRACKING INDIVIDUAL ACTIVITY, BEHAVIOR, OR LOCATION; AND ANY INFORMATION OR DATA DERIVED THEREFROM;

(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[.]; **OR**

(iii) GENETIC INFORMATION WITH RESPECT TO AN INDIVIDUAL, INCLUDING AN INDIVIDUAL’S GENETIC SAMPLE; AN INDIVIDUAL’S

GENETIC TESTS; THE GENETIC TESTS OF FAMILY MEMBERS OF THE INDIVIDUAL; THE MANIFESTATION OF A DISEASE OR DISORDER IN FAMILY MEMBERS OF SUCH INDIVIDUAL; ANY REQUEST FOR, OR RECEIPT OF, A GENETIC TEST, GENETIC COUNSELING, OR GENETIC EDUCATION; AND ANY INFORMATION OR DATA DERIVED THEREFROM.

(iv) NON-PUBLIC SOCIAL MEDIA INFORMATION ABOUT AN INDIVIDUAL, INCLUDING COMMUNICATIONS, POSTINGS, PICTURES, VIDEOS, CONNECTIONS BETWEEN INDIVIDUALS, CONNECTIONS BETWEEN ACCOUNTS, AND ACTIONS.

(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) "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, **MAINTAINS**, 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 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 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 personal information of the individual has been or will be misused as a result of the breach.

(2) [If, after the investigation is concluded,] **UNLESS** the business **REASONABLY** determines that the breach of the security of the system **DOES NOT** create[s] a likelihood that personal information has been or will be misused, 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 **10[45]** days after the business **DISCOVERS OR IS NOTIFIED OF THE BREACH OF THE SECURITY OF A SYSTEM** [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 **3[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.

(d) (1) The notification required under subsection[s] (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 1[30] day[s] 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 **SHALL** [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; **OR**

(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) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION SHALL ALSO BE GIVEN BY[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) 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 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.

(1) THE NOTICE REQUIRED BY THIS SUBSECTION SHALL INCLUDE, AT A MINIMUM: (I) THE NUMBER OF AFFECTED INDIVIDUALS RESIDING IN THE STATE; (II) A DESCRIPTION OF THE BREACH OF THE SECURITY OF A SYSTEM, INCLUDING HOW IT OCCURRED AND ANY VULNERABILITIES THAT WERE EXPLOITED; (III) ANY STEPS THE BUSINESS HAS TAKEN OR PLANS TO TAKE RELATING TO THE BREACH OF THE SECURITY OF A SYSTEM; AND (IV) A SAMPLE OF EACH FORM NOTICE THAT WILL BE SENT TO CONSUMERS PURSUANT TO SUBSECTIONS (E) AND (F).

(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.

§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, 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) or (d)(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.

(d) (1) A business that is subject to and in compliance with the federal Health Insurance Portability and Accountability Act of 1996 shall be deemed to be in compliance with this subtitle.

(2) An affiliate that is in compliance with the federal Health Insurance Portability and Accountability Act of 1996 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.