GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Attorney General

2019 MAR 21 PM 3:31

OFFICE OF THE SECRETARY

ATTORNEY GENERAL
KARL A. RACINE

March 21, 2019

The Honorable Phil Mendelson
Chairman, Council of the District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, N.W.
Suite 504
Washington, DC 20004

Dear Chairman Mendelson:

I am writing to transmit the "Security Breach Protection Amendment Act of 2019". The bill amends Title 28, Chapter 38, Subchapter II of the D.C. Official Code to strengthen the protections for personal information released to unauthorized people because of the breach of the security of a computer system. The bill aims to specify the required contents of a notification of a security breach to a person whose personal information is included in a breach, to clarify timeframes for reporting breaches, to require that written notice of the breach, including specific information, be given to the Office of the Attorney General, to specify the security requirements for the protection of personal information, to make violation of the requirements for protection of personal information an unlawful trade practice, and to require the provision of 2 years of identity theft prevention services when the breach results in the release of social security or tax identification numbers. The bill makes violation of the subchapter a violation of the subchapter an unlawful trade practice subject to the remedies contained in D.C. Official Code § 28-3909.

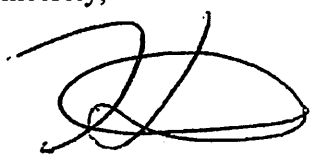
Specifically, the bill:

(1) Updates the definition of personal information to include additional information, including passport number, taxpayer identification number, military ID number, health information, biometric data, genetic information and DNA profiles, and health insurance information;
(2) Inserts requirements for the content of the notification to consumers when there has been a breach, including a requirement that the notification include a statement informing residents of the right to obtain a security freeze at no cost (pursuant to federal law) and information how a resident may request a security freeze, and where appropriate the right to ID theft prevention services as described below;
(3) Requires notification to the Attorney General;

(4) Requires persons and entities that own, license, maintain, license, or otherwise possess personal information to implement and maintain reasonable security procedures and practices;
(5) Adds a requirement that in the case of a breach of SSN, the company must provide 2 years of identity theft prevention services, and
(6) Makes a violation of the data breach law a violation of the CPPA.

If you have any questions, your staff may contact my Legislative Director, James A. Pittman, on (202) 724-6517.

Sincerely,



Karl A. Racine
Attorney General for the District of Columbia

Chairman Phil Mendelson
at the request of the Mayor

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To amend Title 28 of the District of Columbia Official Code concerning businesses' data breaches to expand definitions, to specify the required contents of a notification of a security breach to a person whose personal information is included in a breach, to clarify timeframes for reporting breaches, to require that written notice of the breach, including specific information, be given to the Office of the Attorney General, to specify the security requirements for the protection of personal information, to make violation of the requirements for protection of personal information an unlawful trade practice, and to require the provision of 2 years of identity theft prevention services when the breach results in the release of social security or tax identification numbers.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Security Breach Protection Amendment Act of 2019".

Sec. 2. Title 28, Chapter 38 of the District of Columbia Official Code is amended as follows:

(a) Section 28-3801 is amended by striking the "chapter" and inserting the word "subchapter" in its place.

(b) The table of contents for subchapter II is amended by adding three new section designations to read as follows:

"§ 28-3852a. Security Requirements.

"§ 28-3852b. Remedies.".

"§ 28-3852c. Rulemaking.".

(c) Section 28-3851 is amended as follows:

(1) Paragraph (1) is amended by striking the phrase "shall not be deemed to be a breach of the security of the system" and inserting the phrase "shall not be deemed to be a breach of the security of the system unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access" in its place.

(2) New paragraphs (1A) and (1B) are added to read as follows:

"(1A) Genetic information has the meaning ascribed to it under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), approved August 21, 1996 (Pub. Law 104-191; 110 Stat. 1936), as specified in 45 C.F.R. § 106.103.

"(1B) Medical Information means any information about a consumer's medical or mental health treatment or diagnosis by a health care professional.".

(3) Paragraph (3) is amended to read as follows:

"(3)(A) "Personal information" means:

"(i) An individual's first name, first initial and last name, or any other personal identifier, which, on its own or in combination with any of the following data elements, can be used to identify a person or the person's information:

"(I) Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, military identification number, or other identifier issued by the District of Columbia or any local, state or federal government agency;

"(II) Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account;

"(III) Medical information;

"(IV) Genetic information and deoxyribonucleic acid profile;

"(V) Health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information;

"(VI) 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

"(VII) Any combination of data elements included in sub-sub-sub paragraphs (I) through (VI) of this sub-subparagraph that would be sufficient to permit a person to commit or attempt to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier.

"(ii) A user name or e-mail address in combination with a password, security question and answer or other means of authentication, or any combination of data elements included in sub-sub-sub paragraphs (I) through (VI) that permits access to an individual's e-mail account.".

(d) Section 28-3852 is amended as follows:

(1) A new subsection (a-1) is added to read as follows:

"(a-1) The notification required under subsection (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 the elements of personal information that were, or are reasonably believed to have been, acquired;

"(2) Contact information for the person or entity 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, including a statement notifying the resident of the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may request a security freeze; and

"(4) The toll-free telephone numbers, addresses, and website addresses for the following entities, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft:

"(A) The Federal Trade Commission; and

"(B) The Office of the Attorney General for the District of Columbia.

"(5) Information regarding identity theft protection where when required under 28-3852b.".

(2) New subsections (b-1) and (b-2) are added to read as follows:

"(b-1) Prior to giving the notification required under subsection (a) of this section, and subject to subsection (d) of this section, the person or entity required to give notice shall provide

written notice of the breach of the security system to the Office of the Attorney General. This notice shall include:

"(1) The name and contact information of the person or entity reporting the breach;

"(2) The name and contact information of the person or entity that experienced the breach;

"(3) The nature of the breach of the security of the system, including the name of the person or entity that experienced the breach;

"(4) The types of personal information compromised by the breach;

"(5) The number of District residents affected by the breach;

"(6) The cause of the breach, including the person responsible for the breach, if known;

"(7) Any remedial action taken by the person or entity;

"(8) The date and time frame of the breach, if known; and

"(9) A sample of the notice to be provided to District residents.

"(b-2) The notice required under subsection (b-1) of this section shall not be delayed on the grounds that the total number of District residents affected by the breach has not yet been ascertained.".

(3) Subsection (e) is amended by inserting the following sentence at the end: "The person or entity shall, in all cases, provide written notice of the breach of the security of the system to the Office of the Attorney General as required under subsection (b-1) of this section." in its place.

(4) Subsection (g) is amended by striking the phrase "with this section" and inserting the phrase "with this section with respect to the notification of residents whose personal information is included in the breach. The person or entity shall, in all cases, provide written notice of the breach of the security of the system to the Office of the Attorney General as required under subsection (b-1) of this section" in its place.

(e) New sections 28-3852a, 28-3852b, and 28-3852c are added to read as follows:

"§ 28-3852a. Security requirements.

"(a) To protect personal information from unauthorized access, use, modification, disclosure or a reasonably anticipated hazard or threat, a person or entity that owns, licenses, maintains, handles or otherwise possesses personal information of an individual residing in the District shall implement and maintain reasonable security safeguards, including procedures and practices, that are appropriate to the nature of the personal information and the nature and size of the entity or operation.

"(b) A person or entity that uses a nonaffiliated third party as a service provider to perform services for a person or entity and discloses personal information about an individual residing in the District under a written agreement with the third party shall require by the agreement that the third party implement and maintain reasonable security procedures and practices that:

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

"(2) Are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure.

"(c) When a person or entity is destroying records, including computerized or electronic records and devices containing computerized or electronic records, that contain personal information of a consumer, employee, or former employee of the person or entity, the person or entity 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 and sanitation methods; and

"(4) Available technology.".

"§ 28-3852b. Remedies

"When a person or entity experiences a breach of the security of the system that requires notification under subsection § 28-3852(a) or (b), and such breach includes or is reasonably believed to include a social security number or taxpayer identification number, the person or entity shall offer to each District resident whose social security number or tax identification number was released identity theft protection services at no cost to such District resident for a period of not less than 24 months. The person or entity that experienced the breach of the security of its system shall provide all information necessary for District residents to enroll in the services required under this subsection. This section shall not apply to an action of an agency of government.".

"§ 28-3852c. Rulemaking

The Attorney General for the District of Columbia, pursuant to § 2-501 et seq. may issue rules to implement the provisions of this subchapter.".

(f) Section 28-3853(b) is amended to read as follows:

"(b) A violation of this subchapter, or any rule issued pursuant to the authority of this subchapter, is an unlawful trade practice within the meaning of Chapter 39 of this Title and is subject to the remedies contained in § 28-3909.".

Sec. 3. Fiscal impact statement.

The Council adopts the fiscal impact statement of the Chief Financial Officer as the fiscal impact statement required by section 602(c)(3) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code §1-206.02(c)(3)).

Sec. 4. Effective date.

This act shall take effect following approval by the Mayor (or in the event of veto by the Mayor, action by the Council to override the veto), a 30-day period of congressional review as provided in 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code §1-206.02(c)(1)), and publication in the District of Columbia Register.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL

ATTORNEY GENERAL
KARL A. RACINE

Legal Counsel Division

MEMORANDUM

TO: Alana Intrieri
Executive Director
Office of Policy and Legislative Affairs

FROM: Arthur J. Parker
Acting Deputy Attorney General
Legal Counsel Division

DATE: March 20, 2019

SUBJECT: Legal Sufficiency Certification of the "Security Breach Protection Amendment Act of 2019"
(AL-19-255)

This is to Certify that this Office has reviewed the above-referenced bill and has found it to be legally sufficient. If you have any questions regarding this certification, please do not hesitate to contact me at 724-5565.

Arthur J. Parker