ENGROSSED ORIGINAL

A BILL

23-215

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 require the provision of 18 months of identity theft prevention services when the breach results in the release of social security or tax identification numbers, to make violation of the requirements for protection of personal information an unfair or deceptive trade practice, and to make a conforming amendment to the Consumer Protection Procedures Act.

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 2020".

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

(a) Chapter 38 is amended as follows:

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

(2) The table of contents for subchapter 2 is amended by adding three new section designations to read as follows:

"§ 28-3852a. Security Requirements.

"§ 28-3852b. Remedies.

"§ 28-3852c. Rulemaking.".

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

(A) Paragraph (1) is amended to read as follows:

"(1)(A) "Breach of the security of the system" means unauthorized acquisition of computerized or other electronic data or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or entity who conducts business in the District of Columbia.

"(B) The term "breach of the security of the system" does not include:

"(i) A good faith acquisition of personal information by an employee or agency of the person or entity for the purposes of the person or entity if the personal information is not used improperly or subject to further unauthorized disclosure;

"(ii) Acquisition of data that has been rendered secure, including through encryption or redaction of such data, so as to be unusable by an unauthorized third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access; or

"(iii) Acquisition of personal information of an individual that the person or entity reasonably determines, ~~after consultation with District and federal~~after a reasonable investigation and consultation with the Office of the Attorney General for the District

of Columbia and federal law enforcement agencies, will likely not result in harm to the individual.

(B) 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 dental, medical or mental health treatment or diagnosis by a health care professional.".

(C) Paragraph (2) is amended by striking the word "business" wherever it appears and inserting the word "entity" in its place.

(D) A new paragraph (2A) is added to read as follows:

"(2A) "Person or entity" means an individual, firm, corporation, partnership, company, cooperative, association, trust, or any other organization, legal entity, or group of individuals. The term "person or entity" shall not include the District of Columbia government or any of its agencies or instrumentalities.".

(E) 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, 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, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

"(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 is 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 enable a person 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.".

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

(A) New subsections (a-1) and (a-2) are 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.".

"(a-2) Notwithstanding subsection (a-1), in the case of a breach of the security of the system that only involves personal information defined in section 28-3851(3)(A)(ii), the person or entity may comply with this section by providing the notification in electronic format or other form that directs the person to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the e-mail account with the person or entity and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

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

"(b-1) In addition 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 promptly provide written notice of the breach of the security of the system to the Office of the Attorney General if the breach affects 50 or more District residents. This notice shall be made in the most expedient manner possible, without unreasonable delay, and in no event later than when notice is provided under subsection (a) of this section. The written 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 relationship between the person or entity that experienced the breach and the person responsible for the breach, if known;

"(7) Remedial action taken by the person or entity to include steps taken to assist District residents affected by the breach;

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

"(9) Address and location of corporate headquarters, if outside of the District;

"(10) Any knowledge of foreign country involvement; and

"(11) 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.".

(C) Subsection (e) is repealed.

(D) Subsection (g) is amended to read as follows:

"(g) A person or entity who maintains procedures for a breach notification system under Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 *et seq.*), or the breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability Accountability Act of 1996 (Public Law 104-191), or the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5), and provides notice in accordance with such Acts, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance 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.".

(5) New sections 28-3852a and 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, and 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.

"(d) A person or entity who is subject to and in compliance with requirements for security procedures and practices contained in Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 *et seq*.), or the Health Insurance Portability Accountability Act of 1996 (Public Law 104-191), or the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5), and any rules, regulations, guidance and guidelines thereto, shall be deemed to be in compliance with this section.".

"§ 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 18 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.

"§ 28-3852c. Rulemaking.

"The Attorney General for the District of Columbia, pursuant to section 2-501 *et seq*. may issue rules to implement the notification provisions pursuant to ~~section 28-3852~~ section 28-3852(b-1).".

(6) Section 28-3853 is amended as follows:

(A) Subsection (a) is repealed.

(B) Subsection (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 unfair or deceptive trade practice pursuant to section 28-3904(kk).".

(b) Chapter 39 is amended as follows:

(1) Section 28-3904 is amended as follows:

(A) Subsection (ii) is amended by striking the word "or".

(B) Subsection (jj) is amended by striking the period and inserting the phrase "; or" in its place.

(C) A new subsection (kk) is added to read as follows:

"(kk) violate any provision of subchapter 2 of Chapter 38 of this title.".

(2) Section 28-3905(k)(2)(A) is amended to read as follows:

"(A)(i) Treble damages, or $1,500 per violation, whichever is greater, payable to the consumer;

"(ii) Notwithstanding sub-subparagraph (i) of this subparagraph, for a violation of section 28-3904(kk) a consumer may recover or obtain actual damages, or $250 per violation, whichever is greater;".

~~(2)~~(3) Section 28-3909 is amended by striking the phrase "28-3819 or 28-3904" wherever it appears and inserting the phrase "28-3819, 28-3851, 28-3852, 28-3852a, 28-3852b or 28-3904" in its place.

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.