

AN ACT

D.C. ACT 23-268

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

MARCH 26, 2020

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 time frames for reporting breaches, to require that written notice of a breach, including specific information, be given to the Office of the Attorney General for the District of Columbia, to specify the security requirements for the protection of personal information, to require the provision of 18 months of identity theft prevention services when a breach results in the release of social security or tax identification numbers, and to make violation of the requirements for protection of personal information an unfair or deceptive trade practice.

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) The table of contents is amended by adding new section designations to read as follows:

"§ 28-3852a. Security Requirements.

"§ 28-3852b. Remedies.

"§ 28-3852c. Rulemaking."

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

(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 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