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.

1

30   "§ 28-3852b. Remedies.".

31   "§ 28-3852c. Rulemaking.".

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

33   (1) Paragraph (1) is amended by striking the phrase "shall not be deemed to be a

34   breach of the security of the system" and inserting the phrase "shall not be deemed to be a breach

35   of the security of the system unless any information obtained has the potential to compromise the

36   effectiveness of the security protection preventing unauthorized access" in its place.

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

38   "(1A) Genetic information has the meaning ascribed to it under the federal Health

39   Insurance Portability and Accountability Act of 1996 ("HIPAA"), approved August 21, 1996

40   (Pub. Law 104-191; 110 Stat. 1936), as specified in 45 C.F.R. § 106.103.

41   "(1B) Medical Information means any information about a consumer's medical or

42   mental health treatment or diagnosis by a health care professional.".

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

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

45   "(i) An individual's first name, first initial and last name, or any

46   other personal identifier, which, on its own or in combination with any of the following data

47   elements, can be used to identify a person or the person's information:

48   "(I) Social security number, Individual Taxpayer

49   Identification Number, passport number, driver's license number, military identification number,

50   or other identifier issued by the District of Columbia or any local, state or federal government

51   agency;

2

52   "(II) Account number, credit card number or debit card

53   number, or any other number or code or combination of numbers or codes, such as an

54   identification number, account number, security code, access code, or password, that allows

55   access to or use of an individual's financial or credit account;

56   "(III) Medical information;

57   "(IV) Genetic information and deoxyribonucleic acid

58   profile;

59   "(V) Health insurance information, including a policy

60   number, subscriber information number, or any unique identifier used by a health insurer to

61   identify the person that permits access to an individual's health and billing information;

62   "(VI) Biometric data of an individual generated by

63   automatic measurements of an individual's biological characteristics such as a fingerprint, voice

64   print, genetic print, retina or iris image, or other unique biological characteristic, that can be used

65   to uniquely authenticate the individual's identity when the individual accesses a system or

66   account; or

67   "(VII) Any combination of data elements included in sub-

68   sub-sub paragraphs (I) through (VI) of this sub-subparagraph that would be sufficient to permit a

69   person to commit or attempt to commit identity theft without reference to a person's first name

70   or first initial and last name or other independent personal identifier.

71   "(ii) A user name or e-mail address in combination with a

72   password, security question and answer or other means of authentication, or any combination of

73   data elements included in sub-sub-sub paragraphs (I) through (VI) that permits access to an

74   individual's e-mail account.".

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

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

77   "(a-1) The notification required under subsection (a) of this section shall include:

78   "(1) To the extent possible, a description of the categories of information that

79   were, or are reasonably believed to have been, acquired by an unauthorized person, including the

80   elements of personal information that were, or are reasonably believed to have been, acquired;

81   "(2) Contact information for the person or entity making the notification,

82   including the business address, telephone number, and toll-free telephone number if one is

83   maintained;

84   "(3) The toll-free telephone numbers and addresses for the major consumer

85   reporting agencies, including a statement notifying the resident of the right to obtain a security

86   freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may

87   request a security freeze; and

88   "(4) The toll-free telephone numbers, addresses, and website addresses for the

89   following entities, including a statement that an individual can obtain information from these

90   sources about steps to take to avoid identity theft:

91   "(A) The Federal Trade Commission; and

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

93   "(5) Information regarding identity theft protection where when required under

94   28-3852b.".

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

96   "(b-1) Prior to giving the notification required under subsection (a) of this section, and

97   subject to subsection (d) of this section, the person or entity required to give notice shall provide

98   written notice of the breach of the security system to the Office of the Attorney General. This

99   notice shall include:

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

101   breach;

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

103   the breach;

104   "(3) The nature of the breach of the security of the system, including the name of

105   the person or entity that experienced the breach;

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

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

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

109   known;

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

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

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

113   "(b-2) The notice required under subsection (b-1) of this section shall not be delayed on

114   the grounds that the total number of District residents affected by the breach has not yet been

115   ascertained.".

116   (3) Subsection (e) is amended by inserting the following sentence at the end: "The

117   person or entity shall, in all cases, provide written notice of the breach of the security of the

118   system to the Office of the Attorney General as required under subsection (b-1) of this section."

119   in its place.

120   (4) Subsection (g) is amended by striking the phrase "with this section" and

121 inserting the phrase "with this section with respect to the notification of residents whose personal

122 information is included in the breach. The person or entity shall, in all cases, provide written

123 notice of the breach of the security of the system to the Office of the Attorney General as

124 required under subsection (b-1) of this section" in its place.

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

126   "§ 28-3852a. Security requirements.

127   "(a) To protect personal information from unauthorized access, use, modification,

128 disclosure or a reasonably anticipated hazard or threat, a person or entity that owns, licenses,

129 maintains, handles or otherwise possesses personal information of an individual residing in the

130 District shall implement and maintain reasonable security safeguards, including procedures and

131 practices, that are appropriate to the nature of the personal information and the nature and size of

132 the entity or operation.

133   "(b) A person or entity that uses a nonaffiliated third party as a service provider to

134 perform services for a person or entity and discloses personal information about an individual

135 residing in the District under a written agreement with the third party shall require by the

136 agreement that the third party implement and maintain reasonable security procedures and

137 practices that:

138   "(1) Are appropriate to the nature of the personal information disclosed to the

139 nonaffiliated third party; and

140   "(2) Are reasonably designed to protect the personal information from

141 unauthorized access, use, modification, disclosure.

142   "(c) When a person or entity is destroying records, including computerized or electronic

143 records and devices containing computerized or electronic records, that contain personal

144 information of a consumer, employee, or former employee of the person or entity, the person or

145 entity shall take reasonable steps to protect against unauthorized access to or use of the personal

146 information, taking into account:

147   "(1) The sensitivity of the records;

148   "(2) The nature and size of the business and its operations;

149   "(3) The costs and benefits of different destruction and sanitation methods; and

150   "(4) Available technology.".

151   "§ 28-3852b. Remedies

152   "When a person or entity experiences a breach of the security of the system that requires

153 notification under subsection § 28-3852(a) or (b), and such breach includes or is reasonably

154 believed to include a social security number or taxpayer identification number, the person or

155 entity shall offer to each District resident whose social security number or tax identification

156 number was released identity theft protection services at no cost to such District resident for a

157 period of not less than 24 months. The person or entity that experienced the breach of the

158 security of its system shall provide all information necessary for District residents to enroll in the

159 services required under this subsection. This section shall not apply to an action of an agency of

160 government.".

161   "§ 28-3852c. Rulemaking

162   The Attorney General for the District of Columbia, pursuant to § 2-501 et seq. may issue

163 rules to implement the provisions of this subchapter.".

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

165   "(b) A violation of this subchapter, or any rule issued pursuant to the authority of this

166   subchapter, is an unlawful trade practice within the meaning of Chapter 39 of this Title and is

167   subject to the remedies contained in § 28-3909.".

168   Sec. 3. Fiscal impact statement.

169   The Council adopts the fiscal impact statement of the Chief Financial Officer as the fiscal

170   impact statement required by section 602(c)(3) of the District of Columbia Home Rule Act,

171   approved December 24, 1973 (87 Stat. 813; D.C. Official Code §1-206.02(c)(3)).

172   Sec. 4. Effective date.

173   This act shall take effect following approval by the Mayor (or in the event of veto by the

174   Mayor, action by the Council to override the veto), a 30-day period of congressional review as

175   provided in 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973

176   (87 Stat. 813; D.C. Official Code §1-206.02(c)(1)), and publication in the District of Columbia

177   Register.

178

179