

29 **(HOW IS THIS DIFFERENT?** *This definition would require both the unauthorized*
30 *acquisition **and** access to the data. There may be a situation where someone is able to*
31 *steal the actual data, but also needs some sort of pass key to access it, rendering just the*
32 *data useless. This definition would take into account that situation. Finally, this example*
33 *requires that the data be part of a larger database of personal information about multiple*
34 *people. It would not apply to someone accessing a document or information not*
35 *connected to a database.)*

36

37

38 "Encryption" means the transformation of data through the use of an algorithmic process into a
39 form in which there is low probability of assigning meaning without the use of a confidential process
40 key, or securing the information by another method that renders the data elements unreadable or
41 unusable.

42

43 **Other option:**

- 44 ▪ No definition of "encryption." HB 2721 did not contain such a definition. The effect of
45 no definition would be to assign the term its definition as understood in ordinary usage.

46

47

48 "Entity" means any individual, corporation, partnership, association, cooperative, limited liability
49 company, trust, joint venture, state or local government, political subdivision, or any other legal or any
50 other legal or commercial entity, whether for profit or not-for-profit, or any successor, representative,
51 agent, agency, or instrumentality thereof.

52

53 NOTE: This definition takes into account discussions at the last Privacy Advisory
54 Committee that any approach should treat public & private entities the same.

55

56

57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83

"Notice" means":

1. Written notice to the postal address in the entity's records;

2. Telephone notice;

NOTE: Some suggested legislation does not allow telephone notice as an option

3. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the Uniform Electronic Transactions Act (§ 59.1-479 et seq.); or

NOTE: Some bills do not include the requirement that electronic notice be consistent with UETA, or include the requirement that such notice be consistent with similar federal legislation

4. Substitute notice, if the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the entity does not have sufficient contact information to provide notice as described in subdivisions 1, 2, or 3. Substitute notice consists of any two of the following: (i) e-mail notice if the individual or entity has e-mail addresses for the members of the affected class of individuals; (ii) conspicuous posting of the notice on the Internet site of the entity if the entity maintains an Internet site; and (iii) notice to major statewide media.

Other substitute notice options:

- Various bills set the dollar/number of individuals threshold for substitute notice at different levels. Other options that have been suggested include \$250,000/500,000 persons or \$75,000/100,000 people. Whatever limit is set is a policy decision as to how easy or difficult it should be for an entity to be able to use the substitute notice provisions, instead of individually contacting affected individuals. This policy decision

84 is linked to the Advisory Committee's questions about the burdens this type of legislation
85 would place on businesses.

86

87 NOTE: HB 2721 essentially included a definition of "notice" within the substantive
88 provisions of the bill (see lines 96-105 of HB 2721), by setting forth how notice
89 may be provided. The description of notice could be either place without making a
90 substantive difference in the bill. This is a stylistic choice that the committee may
91 wish to discuss.

92

93 "Personal information" means an individual's first name or first initial and last name in
94 combination with any one or more of the following data elements, when the name or the data elements
95 are not encrypted: (i) social security number; (ii) driver's license or Virginia identification card number;
96 or (iii) financial account number, credit or debit card number, in combination with any security code,
97 access code, or password that would permit access to an individual's financial account. For purposes of
98 this section, "personal information" does not include publicly available information that is lawfully
99 made available to the general public from federal, state, or local government records.

100

101 **Other options for "personal information:"**

- 102
 - Line 75, after combination with, insert "and linked to"

103 *(**WHAT DOES THIS DO?** This would make the section only apply to databases where the*
104 *data fields are linked to one another. For example, in a data base, my first name (Lisa),*
105 *last name (Wallmeyer), street number (910), and street name (Capitol Street) may all be*
106 *separate data fields. It is possible to set up a data base such that these fields are not*
107 *linked to one another...i.e., someone who accesses a database would not be able to link a*
108 *list of last names with a list of first names, a street number with a street name, or that*
109 *same address with a name. It can be argued that if the data is not linked, it is rendered*
110 *useless to an unauthorized user, and thus access to unlinked data should not trigger*
111 *notification requirements.)*

112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137

- Line 76, after encrypted, insert ", redacted or secured by any other method or technology that renders the personal information unreadable or unusable
*(**WHAT DOES THIS DO?** Adding this to the definition would mean that notice would not be triggered if someone accessed a name along with a Social Security Number that had its first five digits redacted. It also takes into account that technologies might emerge other than encryption, and tries to take these future developments into account. If the language referring to redacting information is adopted, then it may also be necessary to add a definition of "redact" (alteration or truncation of data such that no more than the last four digits of a Social Security Number, driver's license number, Virginia identification card number, or financial account number is accessible as part of the personal information.))*

B. Any entity that owns or licenses computerized data that includes personal information about residents of the Commonwealth shall provide notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the Commonwealth who unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Except as provided in subsection D or in order to take any measures necessary to determine the scope of the breach or to restore the reasonable integrity of a data system, notice of the breach shall be given without unreasonable delay.

Other options for subsection B:

- Line 125, after entity that, insert "that conducts business in the Commonwealth and"
- Line 129: after acquired by, insert "and accessed."

138 ▪ Line 129, after unauthorized person, insert "and that causes, or the individual or entity
139 reasonably believes has caused or will cause, identity theft or other fraud or physical
140 harm to any resident of the Commonwealth.

141 *(**WHAT DOES THIS DO?** This changes the standard for when notice must be given. Instead
142 of just looking at whether a breach occurred, an entity would also look at the
143 circumstances surrounding the breach. If the entity concluded that identity theft was
144 reasonably likely, then it would give notice.)*

145
146 ▪ Line 129, after unauthorized person, insert "An entity must also disclose a breach in the
147 security of the system if encrypted information was accessed or acquired in an
148 unencrypted form, or if the security breach involves a person with unauthorized access to
149 the encryption key."

150 *(**WHAT DOES THIS DO?** If encrypted data is not subject to the disclosure requirements, this
151 deals with a situation where someone is able to unencrypt the data and thus gains access
152 to usable information.)*

153
154 ▪ Replace entire first sentence with: An entity that owns or licenses computerized data that
155 includes personal information about a resident of the Commonwealth shall, when it
156 becomes aware of a breach of the security of the system, conduct in good faith a
157 reasonable and prompt investigation to determine the likelihood that personal information
158 has been or will be misused. If the investigation determines that the misuse of
159 information about a resident of the Commonwealth has occurred or is reasonably likely to
160 occur, the entity shall provide notice as soon as possible to the affected residents.

161 *(**WHAT DOES THIS DO?** This adds an extra layer to the process. It requires the business to
162 investigate when a breach occurs to determine if there is a likelihood that personal
163 information is or will be misused. This might add time to the process; on the other hand,
164 it requires the entity to take active steps to investigate, instead of just reaching a quick
165 conclusion that it's not likely that anything will happen as a result of the breach.)*

166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193

- Line 131: after shall be given, strike "without unreasonable delay" and insert "in the most expedient time possible."

(WHAT DOES THIS DO? Because there is no definition of either term, both standards would be left to interpretation. This is a policy choice as to which phrase better conveys the speed at which an entity must act.)

C. An entity that maintains data that includes personal information that the entity does not own shall notify the owner or licensee of the data of any breach of the security of the data immediately following discovery, if the data was, or was reasonably believed to have been, acquired by an unauthorized person.

NOTE: The same comments as above apply to this section.

Other options:

- Line 176, after unauthorized person, insert "Such an entity shall cooperate with the owner or licensee of the data, including sharing information relevant to the breach."
- Line 174, after security of the data, strike "immediately" and insert "as soon as practicable"

D. Notice required by this section may be delayed if a law-enforcement agency determines and advises the entity that notice will impede a criminal or civil investigation, or homeland or national security. Notice required by this section must be made without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize security.

Other Options:

- 194 ▪ Only allow the law-enforcement delay to apply to criminal investigations, and not civil or
195 matters of security.
- 196
- 197 ▪ Insert language indicating that a delay under this subsection must be made in good faith.
- 198
- 199 ▪ Insert third sentence reading, "However, if after an investigation there is no reasonable
200 belief that the personal information will be used in any unlawful manner, no notification
201 shall be required by this section."
- 202
- 203 ▪ Lines 187, after law-enforcement agency determines, insert "in writing"
- 204
- 205 ▪ Line 188, after that notice will, insert "seriously"
- 206

207 E. Before an entity provides notice to more than 1,000 individuals at any one time pursuant to
208 this section, the entity shall, without unreasonable delay, notify all nationwide consumer reporting
209 agencies, as defined in 15 U.S.C. § 1681a(p), of the timing, content and distribution of the notice,
210 including either the number of individuals to whom the notice was given or the type of notice provided.

211

212 **WHAT DOES THIS DO?** *This puts reporting agencies on alert that a notice has been sent*
213 *out, so that they can prepare for a possible influx of calls from affected individuals for*
214 *credit reports.*

215

216 Alternative suggestions:

- 217
- 218 ▪ Replace subsection E with the following: If an entity, upon providing notice pursuant to
219 this section, indicates that the individual may obtain a copy of his credit report from a
220 consumer reporting agency, the entity shall consult the consumer reporting agency as to
221 the timing, content and distribution.

222 (WHAT DOES THIS DO? *This only requires an entity to notify a consumer reporting agency*
223 *if the notice lets the affected individuals know that they may want to obtain a copy of*
224 *their credit report. There is no requirement that such information be included in the*
225 *notice, but if it is, the credit reporting agencies would want to be prepared to deal with*
226 *the increased volume of requests.)*

- 227
- 228 ▪ Do not include such language in the bill.
- 229

230 F. This section shall not be applicable to an entity that maintains its own notification procedures
231 as part of an information privacy or security policy for the treatment of personal information and is
232 consistent with the timing requirements of this section. Such an entity shall be deemed to be in
233 compliance with this section if the entity notifies affected individuals in accordance with its policies in
234 the event of a breach of the system.

235

236 **Other options:**

- 237 ▪ Also exempt from the scope of the section financial institutions that comply with the
- 238 notification requirements prescribed by the Federal Interagency Guidance on Response
- 239 Programs for Unauthorized Access to Customer Information and Customer Notice
- 240 AND/OR any entity that complies with the rules, regulations, procedures, or guidelines
- 241 established by the entity's primary federal regulator OR state/federal regulator (this would
- 242 include the banking industry, insurance industry, healthcare industry, etc.)

- 243
- 244 ▪ Do not include exemptions
- 245

246 G. A Virginia resident aggrieved by a violation of this section shall be entitled to institute an
247 action to recover damages in the amount of \$100 per violation or actual damages, whichever is greater.
248 If the aggrieved party prevails, he may be awarded reasonable attorney's fees and court costs. The
249 provisions of this section may be enforced by injunction or any other available equitable legal remedy.

250 *NOTE: At issue is whether there should be a private right of action to enforce this*
251 *section, which is a policy decision for the Advisory Committee to consider.*

252
253 **Other options:**

- 254
- 255 ■ Replace subsection G with: A violation of this section that results in injury or loss to a
256 resident of the Commonwealth may be enforced by the Office of the Attorney General.
257 The Office of the Attorney General shall have exclusive authority to bring action and
258 may obtain actual damages or a civil penalty not to exceed \$150,000 per breach of the
259 security of the system, or a series of breaches of a similar nature discovered during a
260 single violation.

261
262
263 #
264