

SENATE BILL NO. 960

102ND GENERAL ASSEMBLY

INTRODUCED BY SENATOR BECK.

3402S.01H

KRISTINA MARTIN, Secretary

AN ACT

To repeal section 407.1500, RSMo, and to enact in lieu thereof one new section relating to the safekeeping of personal information, with an existing penalty provision.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section A. Section 407.1500, RSMo, is repealed and one
2 new section enacted in lieu thereof, to be known as section
3 407.1500, to read as follows:

407.1500. 1. As used in this section, the following
2 terms mean:

3 (1) "Breach of security" or "breach", unauthorized
4 access to and unauthorized acquisition of personal
5 information maintained in computerized form by a person that
6 compromises the security, confidentiality, or integrity of
7 the personal information. Good faith acquisition of
8 personal information by a person or that person's employee
9 or agent for a legitimate purpose of that person is not a
10 breach of security, provided that the personal information
11 is not used in violation of applicable law or in a manner
12 that harms or poses an actual threat to the security,
13 confidentiality, or integrity of the personal information;

14 (2) "Consumer", an individual who is a resident of
15 this state;

16 (3) "Consumer reporting agency", the same as defined
17 by the federal Fair Credit Reporting Act, 15 U.S.C. Section
18 1681a;

EXPLANATION-Matter enclosed in bold-faced brackets [thus] in this bill is not enacted and is intended to be omitted in the law.

19 (4) "Encryption", the use of an algorithmic process to
20 transform data into a form in which the data is rendered
21 unreadable or unusable without the use of a confidential
22 process or key;

23 (5) "Health insurance information", an individual's
24 health insurance policy number or subscriber identification
25 number, any unique identifier used by a health insurer to
26 identify the individual;

27 (6) "Medical information", any information regarding
28 an individual's medical history, mental or physical
29 condition, or medical treatment or diagnosis by a health
30 care professional;

31 (7) "Owns or licenses" includes, but is not limited
32 to, personal information that a business retains as part of
33 the internal customer account of the business or for the
34 purpose of using the information in transactions with the
35 person to whom the information relates;

36 (8) "Person", any individual, corporation, business
37 trust, estate, trust, partnership, limited liability
38 company, association, joint venture, government,
39 governmental subdivision, governmental agency, governmental
40 instrumentality, public corporation, or any other legal or
41 commercial entity;

42 (9) "Personal information", an individual's first name
43 or first initial and last name in combination with any one
44 or more of the following data elements that relate to the
45 individual if any of the data elements are not encrypted,
46 redacted, or otherwise altered by any method or technology
47 in such a manner that the name or data elements are
48 unreadable or unusable:

49 (a) Social Security number;

50 (b) Driver's license number or other unique
51 identification number created or collected by a government
52 body;

53 (c) Financial account number, credit card number, or
54 debit card number in combination with any required security
55 code, access code, or password that would permit access to
56 an individual's financial account;

57 (d) Unique electronic identifier or routing code, in
58 combination with any required security code, access code, or
59 password that would permit access to an individual's
60 financial account;

61 (e) Medical information; or

62 (f) Health insurance information.

63 "Personal information" does not include information that is
64 lawfully obtained from publicly available sources, or from
65 federal, state, or local government records lawfully made
66 available to the general public;

67 (10) "Redacted", altered or truncated such that no
68 more than five digits of a Social Security number or the
69 last four digits of a driver's license number, state
70 identification card number, or account number is accessible
71 as part of the personal information.

72 2. (1) Any person that owns or licenses personal
73 information of residents of Missouri or any person that
74 conducts business in Missouri that owns or licenses personal
75 information in any form of a resident of Missouri shall
76 provide notice to the affected consumer that there has been
77 a breach of security following discovery or notification of
78 the breach. The disclosure notification shall be:

79 (a) Made **[without unreasonable delay] within fourteen**
80 **business days of the discovery or notification of the breach;**

81 (b) Consistent with the legitimate needs of law
82 enforcement, as provided in this section; and

83 (c) Consistent with any measures necessary to
84 determine sufficient contact information and to determine
85 the scope of the breach and restore the reasonable
86 integrity, security, and confidentiality of the data system.

87 (2) Any person that maintains or possesses records or
88 data containing personal information of residents of
89 Missouri that the person does not own or license, or any
90 person that conducts business in Missouri that maintains or
91 possesses records or data containing personal information of
92 a resident of Missouri that the person does not own or
93 license, shall notify the owner or licensee of the
94 information of any breach of security immediately following
95 discovery of the breach, consistent with the legitimate
96 needs of law enforcement as provided in this section.

97 (3) The notice required by this section may be delayed
98 if a law enforcement agency informs the person that
99 notification may impede a criminal investigation or
100 jeopardize national or homeland security, provided that such
101 request by law enforcement is made in writing or the person
102 documents such request contemporaneously in writing,
103 including the name of the law enforcement officer making the
104 request and the officer's law enforcement agency engaged in
105 the investigation. The notice required by this section
106 shall be provided [without unreasonable delay] **within**
107 **fourteen business days** after the law enforcement agency
108 communicates to the person its determination that notice
109 will no longer impede the investigation or jeopardize
110 national or homeland security.

111 (4) The notice shall at minimum include a description
112 of the following:

- 113 (a) The incident in general terms;
- 114 (b) The type of personal information that was obtained
115 as a result of the breach of security;
- 116 (c) A telephone number that the affected consumer may
117 call for further information and assistance, if one exists;
- 118 (d) Contact information for consumer reporting
119 agencies;
- 120 (e) Advice that directs the affected consumer to
121 remain vigilant by reviewing account statements and
122 monitoring free credit reports.
- 123 (5) Notwithstanding subdivisions (1) and (2) of this
124 subsection, notification is not required if, after an
125 appropriate investigation by the person or after
126 consultation with the relevant federal, state, or local
127 agencies responsible for law enforcement, the person
128 determines that a risk of identity theft or other fraud to
129 any consumer is not reasonably likely to occur as a result
130 of the breach. Such a determination shall be documented in
131 writing and the documentation shall be maintained for five
132 years.
- 133 (6) For purposes of this section, notice to affected
134 consumers shall be provided by one of the following methods:
- 135 (a) Written notice;
- 136 (b) Electronic notice for those consumers for whom the
137 person has a valid email address and who have agreed to
138 receive communications electronically, if the notice
139 provided is consistent with the provisions of 15 U.S.C.
140 Section 7001 regarding electronic records and signatures for
141 notices legally required to be in writing;
- 142 (c) Telephonic notice, if such contact is made
143 directly with the affected consumers; or
- 144 (d) Substitute notice, if:

145 a. The person demonstrates that the cost of providing
146 notice would exceed one hundred thousand dollars; or

147 b. The class of affected consumers to be notified
148 exceeds one hundred fifty thousand; or

149 c. The person does not have sufficient contact
150 information or consent to satisfy paragraphs (a), (b), or
151 (c) of this subdivision, for only those affected consumers
152 without sufficient contact information or consent; or

153 d. The person is unable to identify particular
154 affected consumers, for only those unidentifiable consumers.

155 (7) Substitute notice under paragraph (d) of
156 subdivision (6) of this subsection shall consist of all the
157 following:

158 (a) Email notice when the person has an electronic
159 mail address for the affected consumer;

160 (b) Conspicuous posting of the notice or a link to the
161 notice on the internet website of the person if the person
162 maintains an internet website; and

163 (c) Notification to major statewide media.

164 (8) In the event a person provides notice to more than
165 one thousand consumers at one time pursuant to this section,
166 the person shall notify, without unreasonable delay, the
167 attorney general's office and all consumer reporting
168 agencies that compile and maintain files on consumers on a
169 nationwide basis, as defined in 15 U.S.C. Section 1681a(p),
170 of the timing, distribution, and content of the notice.

171 3. (1) A person that maintains its own notice
172 procedures as part of an information security policy for the
173 treatment of personal information, and whose procedures are
174 otherwise consistent with the timing requirements of this
175 section, is deemed to be in compliance with the notice
176 requirements of this section if the person notifies affected

177 consumers in accordance with its policies in the event of a
178 breach of security of the system.

179 (2) A person that is regulated by state or federal law
180 and that maintains procedures for a breach of the security
181 of the system pursuant to the laws, rules, regulations,
182 guidances, or guidelines established by its primary or
183 functional state or federal regulator is deemed to be in
184 compliance with this section if the person notifies affected
185 consumers in accordance with the maintained procedures when
186 a breach occurs.

187 (3) A financial institution that is:

188 (a) Subject to and in compliance with the Federal
189 Interagency Guidance Response Programs for Unauthorized
190 Access to Customer Information and Customer Notice, issued
191 on March 29, 2005, by the board of governors of the Federal
192 Reserve System, the Federal Deposit Insurance Corporation,
193 the Office of the Comptroller of the Currency, and the
194 Office of Thrift Supervision, and any revisions, additions,
195 or substitutions relating to said interagency guidance; or

196 (b) Subject to and in compliance with the National
197 Credit Union Administration regulations in 12 CFR Part 748;
198 or

199 (c) Subject to and in compliance with the provisions
200 of Title V of the Gramm-Leach-Bliley Financial Modernization
201 Act of 1999, 15 U.S.C. Sections 6801 to 6809;

202 shall be deemed to be in compliance with this section.

203 4. The attorney general shall have [exclusive]
204 authority to bring an action **and any other person may bring**
205 **an action** to obtain actual damages for a willful and knowing
206 violation of this section [and may seek], **but damages shall**
207 **not exceed one hundred fifty thousand dollars per breach of**

208 **the security of the system or series of breaches of a**
209 **similar nature that are discovered in a single**
210 **investigation. Additionally, a civil penalty for a**
211 **violation may be awarded but shall not [to] exceed one**
212 **hundred fifty thousand dollars per breach of the security of**
213 **the system or series of breaches of a similar nature that**
214 **are discovered in a single investigation.**

✓