

FIRST REGULAR SESSION

# HOUSE BILL NO. 35

100TH GENERAL ASSEMBLY

---

INTRODUCED BY REPRESENTATIVE STACY.

0566H.011

DANA RADEMAN MILLER, Chief Clerk

---

## 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 penalty provisions.

---

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

Section A. Section 407.1500, RSMo, is repealed and one new section enacted in lieu thereof, to be known as section 407.1500, to read as follows:

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

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

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

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

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

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

EXPLANATION — Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

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

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

23 (8) "Person", any individual, corporation, business trust, estate, trust, partnership, limited  
24 liability company, association, joint venture, government, governmental subdivision,  
25 governmental agency, governmental instrumentality, public corporation, or any other legal or  
26 commercial entity;

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

31 (a) Social Security number;

32 (b) Driver's license number or other unique identification number created or collected  
33 by a government body;

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

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

40 (e) Medical information; or

41 (f) Health insurance information.

42

43 "Personal information" does not include information that is lawfully obtained from publicly  
44 available sources, or from federal, state, or local government records lawfully made available to  
45 the general public;

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

49 2. (1) Any person that owns or licenses personal information of residents of Missouri  
50 or any person that conducts business in Missouri that owns or licenses personal information in  
51 any form of a resident of Missouri shall provide notice to the affected consumer that there has  
52 been a breach of security following discovery or notification of the breach. The disclosure  
53 notification shall be:

54 (a) Made ~~[without unreasonable delay]~~ **within thirty days of the discovery or**  
55 **notification of the breach;**

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

58 (c) Consistent with any measures necessary to determine sufficient contact information  
59 and to determine the scope of the breach and restore the reasonable integrity, security, and  
60 confidentiality of the data system.

61 (2) Any person that maintains or possesses records or data containing personal  
62 information of residents of Missouri that the person does not own or license, or any person that  
63 conducts business in Missouri that maintains or possesses records or data containing personal  
64 information of a resident of Missouri that the person does not own or license, shall notify the  
65 owner or licensee of the information of any breach of security immediately following discovery  
66 of the breach, consistent with the legitimate needs of law enforcement as provided in this section.

67 (3) The notice required by this section may be delayed if a law enforcement agency  
68 informs the person that notification may impede a criminal investigation or jeopardize national  
69 or homeland security, provided that such request by law enforcement is made in writing or the  
70 person documents such request contemporaneously in writing, including the name of the law  
71 enforcement officer making the request and the officer's law enforcement agency engaged in the  
72 investigation. The notice required by this section shall be provided ~~[without unreasonable delay]~~  
73 **within thirty days** after the law enforcement agency communicates to the person its  
74 determination that notice will no longer impede the investigation or jeopardize national or  
75 homeland security.

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

77 (a) The incident in general terms;

78 (b) The type of personal information that was obtained as a result of the breach of  
79 security;

80 (c) A telephone number that the affected consumer may call for further information and  
81 assistance, if one exists;

82 (d) Contact information for consumer reporting agencies;

83 (e) Advice that directs the affected consumer to remain vigilant by reviewing account  
84 statements and monitoring free credit reports.

85 (5) Notwithstanding subdivisions (1) and (2) of this subsection, notification is not  
86 required if, after an appropriate investigation by the person or after consultation with the relevant  
87 federal, state, or local agencies responsible for law enforcement, the person determines that a risk  
88 of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the

89 breach. Such a determination shall be documented in writing and the documentation shall be  
90 maintained for five years.

91 (6) For purposes of this section, notice to affected consumers shall be provided by one  
92 of the following methods:

93 (a) Written notice;

94 (b) Electronic notice for those consumers for whom the person has a valid email address  
95 and who have agreed to receive communications electronically, if the notice provided is  
96 consistent with the provisions of 15 U.S.C. Section 7001 regarding electronic records and  
97 signatures for notices legally required to be in writing;

98 (c) Telephonic notice, if such contact is made directly with the affected consumers; or

99 (d) Substitute notice, if:

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

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

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

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

109 (7) Substitute notice under paragraph (d) of subdivision (6) of this subsection shall  
110 consist of all the following:

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

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

115 (c) Notification to major statewide media.

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

121 3. (1) A person that maintains its own notice procedures as part of an information  
122 security policy for the treatment of personal information, and whose procedures are otherwise  
123 consistent with the timing requirements of this section, is deemed to be in compliance with the

124 notice requirements of this section if the person notifies affected consumers in accordance with  
125 its policies in the event of a breach of security of the system.

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

131 (3) A financial institution that is:

132 (a) Subject to and in compliance with the Federal Interagency Guidance Response  
133 Programs for Unauthorized Access to Customer Information and Customer Notice, issued on  
134 March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit  
135 Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift  
136 Supervision, and any revisions, additions, or substitutions relating to said interagency guidance;  
137 or

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

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

142

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

144 4. The attorney general shall have exclusive authority to bring an action to obtain actual  
145 damages for a willful and knowing violation of this section and may seek a civil penalty not to  
146 exceed one hundred fifty thousand dollars per breach of the security of the system or series of  
147 breaches of a similar nature that are discovered in a single investigation.

✓