

FIRST REGULAR SESSION
HOUSE COMMITTEE SUBSTITUTE FOR
HOUSE BILL NO. 436
103RD GENERAL ASSEMBLY

1574H.02C

JOSEPH ENGLER, Chief Clerk

AN ACT

To amend chapter 375, RSMo, by adding thereto twelve new sections relating to insurance companies' data security, with penalty provisions.

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

Section A. Chapter 375, RSMo, is amended by adding thereto twelve new sections, to
2 be known as sections 375.1400, 375.1402, 375.1405, 375.1407, 375.1410, 375.1412,
3 375.1415, 375.1417, 375.1420, 375.1422, 375.1425, and 375.1427, to read as follows:

**375.1400. 1. Sections 375.1400 to 375.1427 shall be known and may be cited as
2 the "Insurance Data Security Act".**

**3 2. Notwithstanding any other provision of law, sections 375.1400 to 375.1427
4 establish the exclusive state standards applicable to licensees for data security, the
5 investigation of a cybersecurity event as defined in section 375.1402, and notification to
6 the director.**

**7 3. Sections 375.1400 to 375.1427 shall not be construed to create or imply a
8 private cause of action for violation of their provisions, nor shall such sections be
9 construed to curtail a private cause of action that would otherwise exist in the absence of
10 sections 375.1400 to 375.1427.**

375.1402. 1. As used in sections 375.1400 to 375.1427, the following terms mean:

**2 (1) "Authorized person", an individual known to and authorized by the licensee
3 and determined to be necessary and appropriate to have access to the nonpublic
4 information held by the licensee and its information systems;**

**5 (2) "Consumer", an individual, including, but not limited to, applicants,
6 policyholders, insureds, beneficiaries, claimants, and certificate holders, who is a**

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.

7 resident of this state and whose nonpublic information is in a licensee's possession,
8 custody, or control;

9 (3) "Cybersecurity event", an event resulting in unauthorized access to,
10 malicious disruption of, or misuse of an information system or nonpublic information in
11 the possession, custody, or control of a licensee or an authorized person; however:

12 (a) The term "cybersecurity event" does not include the unauthorized
13 acquisition of encrypted, nonpublic information if the encryption, process, or key is
14 not also acquired, released, or used without authorization; and

15 (b) The term "cybersecurity event" does not include an event with regard to
16 which the licensee has determined that the nonpublic information accessed by an
17 unauthorized person has not been used or released and has been returned or destroyed;

18 (4) "Department", the department of commerce and insurance;

19 (5) "Director", the director of the department of commerce and insurance;

20 (6) "Encrypted", the transformation of data into a form that results in a low
21 probability of assigning meaning without the use of a protective process or key;

22 (7) "HIPAA", the federal Health Insurance Portability and Accountability Act
23 (42 U.S.C. Section 1320d et seq.);

24 (8) "Information security program", the administrative, technical, and physical
25 safeguards that a licensee uses to access, collect, distribute, process, protect, store, use,
26 transmit, dispose of, or otherwise handle nonpublic information;

27 (9) "Information system", a discrete set of electronic information resources
28 organized for the collection, processing, maintenance, use, sharing, dissemination, or
29 disposition of electronic nonpublic information, as well as any specialized system such as
30 industrial and process controls systems, telephone switching and private branch
31 exchange systems, and environmental control systems;

32 (10) "Licensee", any person licensed, authorized to operate, or registered, or
33 required to be licensed, authorized, or registered under the insurance laws of this state,
34 but shall not include a purchasing group or a risk retention group chartered and
35 licensed in a state other than this state or a licensee that is acting as an assuming insurer
36 that is domiciled in another state or jurisdiction;

37 (11) "Multi-factor authentication", authentication through verification of at
38 least two of the following types of authentication factors:

39 (a) Knowledge factors, such as a password;

40 (b) Possession factors, such as a token or text message on a mobile phone; or

41 (c) Inherence factors, such as a biometric characteristic;

42 (12) "Nonpublic information", information that is not publicly available
43 information and is:

44 (a) Business-related information of a licensee, the tampering with which, or
45 unauthorized disclosure, access, or use of which, would cause a material adverse impact
46 to the business, operations, or security of the licensee;

47 (b) Any information concerning a consumer that, because of name, number,
48 personal mark, or other identifier, can be used to identify such consumer, in
49 combination with any one or more of the following data elements:

50 a. Social Security number;

51 b. Driver's license number or nondriver identification card number;

52 c. Financial account number or credit or debit card number;

53 d. Any security code, access code, or password that would permit access to a
54 consumer's financial account;

55 e. Biometric records; or

56 f. Military identification number;

57 (c) Any information or data, except age or gender, in any form or medium
58 created by or derived from a health care provider or a consumer and that relates to:

59 a. The past, present, or future physical, mental, or behavioral health or
60 condition of any consumer or a member of the consumer's family;

61 b. The provision of health care to any consumer; or

62 c. Payment for the provision of health care to any consumer;

63 (13) "Person", any individual or any nongovernmental entity including, but not
64 limited to, any nongovernmental partnership, corporation, branch, agency, or
65 association;

66 (14) "Publicly available information", any information that a licensee has a
67 reasonable basis to believe is lawfully made available to the general public from federal,
68 state, or local government records; widely distributed media; or disclosures to the
69 general public that are required to be made by federal, state, or local law. For the
70 purposes of this definition, a licensee has a reasonable basis to believe that information
71 is lawfully made available to the general public if the licensee has taken steps to
72 determine:

73 (a) That the information is of the type that is available to the general public; and

74 (b) Whether a consumer can direct that the information not be made available to
75 the general public and, if so, that such consumer has not done so;

76 (15) "Risk assessment", the risk assessment that each licensee is required to
77 conduct under subsection 3 of section 375.1405;

78 (16) "State", the state of Missouri;

79 (17) "Third-party service provider", a person, not otherwise defined as a
80 licensee, that contracts with a licensee to maintain, process, store, or otherwise is

81 permitted access to nonpublic information through its provision of services to the
82 licensee.

375.1405. 1. Commensurate with the size and complexity of the licensee; the
2 nature and scope of the licensee's activities, including its use of third-party service
3 providers; and the sensitivity of the nonpublic information used by the licensee or in the
4 licensee's possession, custody, or control, each licensee shall develop, implement, and
5 maintain a comprehensive written information security program that is based on the
6 licensee's risk assessment and that contains administrative, technical, and physical
7 safeguards for the protection of nonpublic information and the licensee's information
8 system.

9 2. A licensee's information security program shall be designed to:

10 (1) Protect the security and confidentiality of nonpublic information and the
11 security of the information system;

12 (2) Protect against any threats or hazards to the security or integrity of
13 nonpublic information and the information system;

14 (3) Protect against unauthorized access to or use of nonpublic information and
15 minimize the likelihood of harm to any consumer; and

16 (4) Define and periodically reevaluate a schedule for retention of nonpublic
17 information and a mechanism for its destruction when no longer needed.

18 3. The licensee shall:

19 (1) Designate one or more employees, an affiliate, or an outside vendor
20 designated to act on behalf of the licensee who is responsible for the information security
21 program;

22 (2) Identify reasonably foreseeable internal or external threats that could result
23 in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of
24 nonpublic information, including the security of information systems and nonpublic
25 information that are accessible to, or held by, third-party service providers;

26 (3) Assess the likelihood and potential damage of these threats, taking into
27 consideration the sensitivity of the nonpublic information;

28 (4) Assess the sufficiency of policies, procedures, information systems, and other
29 safeguards in place to manage these threats, including consideration of threats in each
30 relevant area of the licensee's operations, including:

31 (a) Employee training and management;

32 (b) Information systems, including network and software design, as well as
33 information classification, governance, processing, storage, transmission, and disposal;

34 and

35 (c) Detecting, preventing, and responding to attacks, intrusions, or other systems
36 failures; and

37 (5) Implement information safeguards to manage the threats identified in its
38 ongoing assessment, and no less than annually, assess the effectiveness of the safeguards'
39 key controls, systems, and procedures.

40 4. Based on its risk assessment, the licensee shall:

41 (1) Design its information security program to mitigate the identified risks,
42 commensurate with the size and complexity of the licensee's activities, including its use
43 of third-party service providers, and the sensitivity of the nonpublic information used
44 by the licensee or in the licensee's possession, custody, or control;

45 (2) Determine which of the following security measures are appropriate and
46 implement such security measures:

47 (a) Place access controls on information systems, including controls to
48 authenticate and permit access only to authorized persons to protect against the
49 unauthorized acquisition of nonpublic information;

50 (b) Identify and manage the data, personnel, devices, systems, and facilities that
51 enable the organization to achieve business purposes in accordance with their relative
52 importance to business objectives and the organization's risk strategy;

53 (c) Restrict access at physical locations containing nonpublic information only to
54 authorized persons;

55 (d) Protect by encryption or other appropriate means all nonpublic information
56 while being transmitted over an external network and all nonpublic information stored
57 on a laptop computer or other portable computing or storage device or media;

58 (e) Adopt secure development practices for in-house developed applications
59 utilized by the licensee and procedures for evaluating, assessing, or testing the security
60 of externally developed applications utilized by the licensee;

61 (f) Modify the information system in accordance with the licensee's information
62 security program;

63 (g) Utilize effective controls, which may include multi-factor authentication
64 procedures for any individual accessing nonpublic information;

65 (h) Regularly test and monitor systems and procedures to detect actual and
66 attempted attacks on, or intrusions into, information systems;

67 (i) Include audit trails within the information security program designed to
68 detect and respond to cybersecurity events and designed to reconstruct material
69 financial transactions sufficient to support normal operations and obligations of the
70 licensee;

(j) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(k) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format;

(3) Include cybersecurity risks in the licensee's enterprise risk management process;

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

5. If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program;

(2) Require the licensee's executive management or its delegates to report in writing, at least annually, the following information:

(a) The overall status of the information security program and the licensee's compliance with sections 375.1400 to 375.1427; and

(b) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program;

(3) If executive management delegates any of its responsibilities under section 375.1405, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and shall receive a report from the delegates complying with the requirements of the report to the board of directors above.

6. (1) A licensee shall exercise due diligence in selecting its third-party service provider.

(2) A licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

107 7. The licensee shall monitor, evaluate, and adjust, as appropriate, the
108 information security program consistent with any relevant changes in technology, the
109 sensitivity of its nonpublic information, internal or external threats to information, and
110 the licensee's own changing business arrangements, such as mergers and acquisitions,
111 alliances and joint ventures, outsourcing arrangements, and changes to information
112 systems.

113 8. As part of its information security program, each licensee shall establish a
114 written incident response plan designed to promptly respond to, and recover from, any
115 cybersecurity event that compromises the confidentiality, integrity, or availability of
116 nonpublic information in its possession, the licensee's information systems, or the
117 continuing functionality of any aspect of the licensee's business or operations. Such
118 incident response plan shall address the following areas:

- 119 (1) The internal process for responding to a cybersecurity event;
- 120 (2) The goals of the incident response plan;
- 121 (3) The definition of clear roles, responsibilities, and levels of decision-making
122 authority;
- 123 (4) External and internal communications and information sharing;
- 124 (5) Identification of requirements for the remediation of any identified
125 weaknesses in information systems and associated controls;
- 126 (6) Documentation and reporting regarding cybersecurity events and related
127 incident response activities; and
- 128 (7) The evaluation and revision as necessary of the incident response plan
129 following a cybersecurity event.

130 9. Annually by April fifteenth, each insurer domiciled in this state shall submit
131 to the director a written statement certifying that the insurer is in compliance with the
132 requirements set forth in this section. Each insurer shall maintain for examination by
133 the department all records, schedules, and data supporting this certificate for a period
134 of five years. To the extent an insurer has identified areas, systems, or processes that
135 require material improvement, updating, or redesign, the insurer shall document the
136 identification and the remedial efforts planned and underway to address such areas,
137 systems, or processes. Such documentation shall be available for inspection by the
138 director.

375.1407. 1. If the licensee learns that a cybersecurity event has or may have
2 occurred, the licensee, or an outside vendor or service provider designated to act on
3 behalf of the licensee, shall conduct a prompt investigation.

4 **2. During the investigation, the licensee, or an outside vendor or service provider**
5 **designated to act on behalf of the licensee, shall, at a minimum, determine as much of**
6 **the following information as practicable:**

7 **(1) Determine whether a cybersecurity event has occurred;**

8 **(2) Assess the nature and scope of the cybersecurity event;**

9 **(3) Identify any nonpublic information that may have been involved in the**
10 **cybersecurity event; and**

11 **(4) Perform or oversee reasonable measures to restore the security of the**
12 **information systems compromised in the cybersecurity event in order to prevent further**
13 **unauthorized acquisition, release, or use of nonpublic information in the licensee's**
14 **possession, custody, or control.**

15 **3. If the licensee learns that a cybersecurity event has or may have occurred in a**
16 **system maintained by a third-party service provider, the licensee shall complete the**
17 **steps listed in subsection 2 of this section or confirm and document that the third-party**
18 **service provider has completed those steps.**

19 **4. The licensee shall maintain records concerning all cybersecurity events for a**
20 **period of at least three years from the date of the cybersecurity event and shall produce**
21 **those records upon demand of the director.**

375.1410. 1. Each licensee shall notify the director as promptly as practicable,
2 **but in no event later than four business days, from a determination that a cybersecurity**
3 **event involving nonpublic information that is in the possession of a licensee has occurred**
4 **when either of the following criteria has been met:**

5 **(1) This state is the licensee's state of domicile, in the case of an insurer, or this**
6 **state is the licensee's home state, in the case of a producer, as those terms are defined in**
7 **section 375.012, and the cybersecurity event has a reasonable likelihood of materially**
8 **harming a consumer residing in this state or a reasonable likelihood of materially**
9 **harming any material part of the normal operations of the licensee; or**

10 **(2) The licensee reasonably believes that the nonpublic information involved is of**
11 **two hundred fifty or more consumers residing in this state and is either of the following:**

12 **(a) A cybersecurity event impacting the licensee of which notice is required to be**
13 **provided to any government body, self-regulatory agency, or any other supervisory body**
14 **under any state or federal law; or**

15 **(b) A cybersecurity event that has a reasonable likelihood of materially**
16 **harming:**

17 **a. Any consumer residing in this state; or**

18 **b. Any material part of the normal operations of the licensee.**

- 19 **2. The licensee shall provide as much of the following information as practicable**
20 **except that the licensee shall not release to the state or any other entity nonpublic**
21 **information of the consumer unless given written authority by the consumer or**
22 **otherwise required by law. The licensee shall provide the information in electronic form**
23 **as directed by the director. The licensee shall have a continuing obligation to update**
24 **and supplement initial and subsequent notifications to the director regarding material**
25 **changes to previously provided information relating to the cybersecurity event:**
- 26 **(1) The date of the cybersecurity event;**
27 **(2) A description of how the information was exposed, lost, stolen, or breached,**
28 **including the specific roles and responsibilities of third-party service providers, if any;**
29 **(3) How the cybersecurity event was discovered;**
30 **(4) Whether any exposed, lost, stolen, or breached information has been**
31 **recovered and if so, how this was done;**
32 **(5) The identity of the source of the cybersecurity event;**
33 **(6) Whether the licensee has filed a police report or has notified any regulatory,**
34 **government, or law enforcement agencies and, if so, when such notification was**
35 **provided;**
36 **(7) A description of the specific types of information acquired without**
37 **authorization. "Specific types of information" means particular data elements**
38 **including, for example, types of medical information, types of financial information,**
39 **or types of information allowing identification of the consumer;**
40 **(8) The period during which the information system was compromised by the**
41 **cybersecurity event;**
42 **(9) The number of total consumers in this state affected by the cybersecurity**
43 **event. The licensee shall provide the best estimate in the initial report to the director**
44 **and update this estimate with each subsequent report to the director under this section;**
45 **(10) The results of any internal review identifying a lapse in either automated**
46 **controls or internal procedures, or confirming that all automated controls or internal**
47 **procedures were followed;**
48 **(11) A description of the efforts being undertaken to remediate the situation that**
49 **permitted the cybersecurity event to occur;**
50 **(12) A copy of the licensee's privacy policy and a statement outlining the steps**
51 **the licensee will take to investigate and notify consumers affected by the cybersecurity**
52 **event; and**
53 **(13) The name of a contact person who is both familiar with the cybersecurity**
54 **event and authorized to act for the licensee.**

55 3. The licensee shall comply with section 407.1500, as applicable, and provide a
56 copy of the notice sent to consumers under that section to the director when a licensee is
57 required to notify the director under subsection 1 of section 375.1410.

58 4. (1) In the case of a cybersecurity event in a system maintained by a third-
59 party service provider of which the licensee has become aware, the licensee shall treat
60 such event as it would under subsection 1 of section 375.1410.

61 (2) The computation of a licensee's deadlines shall begin on the day after the
62 third-party service provider notifies the licensee of the cybersecurity event or the
63 licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

64 (3) Nothing in sections 375.1400 to 375.1427 shall prevent or abrogate an
65 agreement between a licensee and another licensee, a third-party service provider, or
66 any other party to fulfill any of the investigation requirements imposed under section
67 375.1407 or notice requirements imposed under this section.

68 5. (1) (a) In the event of a cybersecurity event involving nonpublic information
69 that is used by the licensee that is acting as an assuming insurer or in the possession,
70 custody, or control of a licensee that is acting as an assuming insurer and that does not
71 have a direct contractual relationship with the affected consumers, the assuming insurer
72 shall notify its affected ceding insurers and the commissioner or director of insurance
73 for its state of domicile within three business days of making the determination that a
74 cybersecurity event has occurred.

75 (b) The ceding insurers that have a direct contractual relationship with affected
76 consumers shall fulfill the consumer notification requirements imposed under section
77 407.1500 and any other notification requirements relating to a cybersecurity event
78 imposed under this section.

79 (c) Any licensee acting as assuming insurer shall have no other notice obligations
80 relating to a cybersecurity event or other data breach under this section or any other
81 law of the state.

82 (2) (a) In the event of a cybersecurity event involving nonpublic information
83 that is in the possession, custody, or control of a third-party service provider of a
84 licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding
85 insurers and the commissioner or director of insurance for its state of domicile within
86 three business days of receiving notice from its third-party service provider that a
87 cybersecurity event has occurred.

88 (b) The ceding insurers that have a direct contractual relationship with affected
89 consumers shall fulfill the consumer notification requirements imposed under section
90 407.1500 and any other notification requirements relating to a cybersecurity event
91 imposed under this section.

92 **6. In the case of a cybersecurity event involving nonpublic information that is in**
93 **the possession, custody, or control of a licensee that is an insurer or its third-party**
94 **service provider for which a consumer accessed the insurer's services through an**
95 **independent insurance producer, and for which consumer notice is required by law,**
96 **including section 407.1500, the insurer shall notify the producers of record of all affected**
97 **consumers of the cybersecurity event no later than the time at which notice is provided**
98 **to the affected consumers. The insurer is excused from this obligation for those**
99 **instances in which it does not have the current producer of record information for any**
100 **individual consumer.**

375.1412. 1. The director shall have power to examine and investigate the affairs
2 **of any licensee to determine whether the licensee has been or is engaged in any conduct**
3 **in violation of sections 375.1400 to 375.1427. This power is in addition to the powers the**
4 **director has under the law. Any such investigation or examination shall be conducted**
5 **under section 374.190 or 374.205.**

6 **2. Whenever the director has reason to believe that a licensee has been or is**
7 **engaged in conduct in this state that violates sections 375.1400 to 375.1427, the director**
8 **may take action that is necessary or appropriate to enforce the provisions of sections**
9 **375.1400 to 375.1427.**

375.1415. 1. Any documents, materials, or other information in the control or
2 **possession of the department that are furnished by a licensee or an employee or agent**
3 **thereof acting on behalf of a licensee under subsection 9 of section 375.1405 or**
4 **subsection 2 of section 375.1410 or that is obtained by the director in an investigation or**
5 **examination under section 375.1412 shall be confidential by law and privileged, shall not**
6 **be subject to disclosure under chapter 610, shall not be subject to subpoena, and shall**
7 **not be subject to discovery or admissible in evidence in any private civil action.**
8 **However, the director is authorized to use the documents, materials, or other**
9 **information in the furtherance of any regulatory or legal action brought as a part of**
10 **the director's duties.**

11 **2. Neither the director nor any person or entity who received documents,**
12 **materials, or other information while acting under the authority of the director shall be**
13 **permitted or required to testify in any private civil action concerning any confidential**
14 **documents, materials, or information subject to subsection 1 of this section.**

15 **3. Consistent with the insurance data security act's goal of safeguarding**
16 **consumer nonpublic information, the director or any person or entity who receives**
17 **documents, materials, or other information while acting under the authority of the**
18 **director under sections 375.1400 to 375.1427 may share such documents, materials, or**
19 **other information with another state or federal governmental agency or officer or the**

20 National Association of Insurance Commissioners; provided that the recipient agrees in
21 writing to maintain the confidentiality of such documents, materials, or other
22 information, and has verified in writing the legal authority to maintain such
23 confidentiality. Except as permitted in this subsection, neither the director nor any
24 person or entity who receives documents, materials, or other information under sections
25 375.1400 to 375.1427 shall be permitted to:

26 (1) Share or otherwise release the documents, materials, or other information to
27 a third party;

28 (2) Share or otherwise release the documents, materials, or other information for
29 commercial use; or

30 (3) Sell cyber event or nonpublic information of any person or entity.

31 4. In order to assist in the performance of the director's duties under sections
32 375.1400 to 375.1427, the director:

33 (1) May receive documents, materials, or information, including otherwise
34 confidential and privileged documents, materials, or information, from the National
35 Association of Insurance Commissioners, its affiliates, or subsidiaries and from
36 regulatory and law enforcement officials of other foreign or domestic jurisdictions
37 and shall maintain as confidential or privileged any document, material, or information
38 received with notice or the understanding that it is confidential or privileged under the
39 laws of the jurisdiction that is the source of the document, material, or information; and

40 (2) May enter into agreements governing sharing and use of information
41 consistent with this subsection.

42 5. No waiver of any applicable privilege or claim of confidentiality in the
43 documents, materials, or information shall occur as a result of disclosure to the director
44 under this section or as a result of sharing as authorized in subsection 3 of this section.

45 6. Nothing in sections 375.1400 to 375.1427 shall prohibit the director from
46 releasing final adjudicated actions that are open to public inspection under chapter 610
47 to a database or other clearinghouse service maintained by the National Association of
48 Insurance Commissioners, its affiliates, or subsidiaries.

375.1417. 1. The following exceptions shall apply to sections 375.1400 to
2 375.1427:

3 (1) A licensee with fewer than ten employees, including any independent
4 contractors, is exempt from the provisions of section 375.1405;

5 (2) A licensee subject to and governed by the privacy, security, and breach
6 notification rules issued by the United States Department of Health and Human
7 Services, 45 CFR 160 and 164, established under the Health Insurance Portability and
8 Accountability Act of 1996, Pub. L. 104-191, and the Health Information Technology for

9 Economic and Clinical Health Act (HITECH), Pub. L. 111-5, and that maintains
10 nonpublic information in the same manner as protected health information shall be
11 deemed to comply with the requirements of sections 375.1400 to 375.1427, except for the
12 director notification requirements in subsections 1 and 2 of section 375.1410;

13 (3) An employee, agent, representative, or designee of a licensee, who is also a
14 licensee, is exempt from section 375.1405 and need not develop its own information
15 security program to the extent that the employee, agent, representative, or designee is
16 covered by the information security program of the other licensee;

17 (4) Producers that have fewer than fifty employees; less than five million dollars
18 in gross annual revenue; or less than ten million dollars in year-end total assets; and

19 (5) A licensee affiliated with a depository institution that maintains an
20 information security program in compliance with the Interagency Guidelines
21 Establishing Standards for Safeguarding Customer Information (Interagency
22 Guidelines) as set forth under Sections 501 and 505 of the federal Gramm-Leach-
23 Bliley Act, Pub. L. 106-102, shall be considered to meet the requirements of section
24 375.1405 and any rules, regulations, or procedures established thereunder, provided
25 that the licensee produces, upon request, documentation satisfactory to the director that
26 independently validates the affiliated depository institution's adoption of an information
27 security program that satisfies the interagency guidelines.

28 2. In the event that a licensee ceases to qualify for an exception, such licensee
29 shall have one hundred eighty calendar days to comply with sections 375.1400 to
30 375.1427.

375.1420. In the case of a violation of sections 375.1400 to 375.1427, a licensee
2 may be subject to penalties as provided by law, including sections 374.046, 374.048, and
3 374.049.

375.1422. The director of the department of commerce and insurance may
2 promulgate rules as necessary for the implementation of sections 375.1400 to 375.1427.
3 Any rule or portion of a rule, as that term is defined in section 536.010, that is created
4 under the authority delegated in this section shall become effective only if it complies
5 with and is subject to all of the provisions of chapter 536 and, if applicable, section
6 536.028. This section and chapter 536 are nonseverable and if any of the powers vested
7 with the general assembly under chapter 536 to review, to delay the effective date, or to
8 disapprove and annul a rule are subsequently held unconstitutional, then the grant of
9 rulemaking authority and any rule proposed or adopted after August 28, 2025, shall be
10 invalid and void.

375.1425. If any provision of sections 375.1400 to 375.1427 or the application
2 thereof to any person or circumstance is for any reason held to be invalid, the remainder

3 of sections 375.1400 to 375.1427 and the application of such provision to other persons
4 or circumstances shall not be affected thereby.

375.1427. Sections 375.1400 to 375.1427 shall take effect on January 1, 2026.
2 Licensees shall have until January 1, 2027, to implement section 375.1405 and until
3 January 1, 2028, to implement subsection 6 of section 375.1405.

✓