THE INSURANCE CODE OF 1956 (EXCERPT)
Act 218 of 1956

500.561 Notice of cybersecurity event to residents of this state; conditions and requirements; duties of licensee; substitute notice; notification to certain consumer reporting agencies; exception; compliance with health insurance portability and accountability act considered compliance with section; notice with intent to defraud; misdemeanor; penalty; failure to provide notice; civil fine; aggregate liability; applicability of section; definitions.

Sec. 561.

(1) Unless the licensee determines that the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a licensee that owns or licenses data that are included in a database that discovers a cybersecurity event, or receives notice of a cybersecurity event under subsection (2), shall provide a notice of the cybersecurity event to each resident of this state who meets 1 or more of the following:

(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.

(b) That resident's personal information was accessed and acquired in encrypted form by a licensee with unauthorized access to the encryption key.

(2) Unless the licensee determines that the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a licensee that maintains a database that includes data that the licensee does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the cybersecurity event.

(3) In determining whether a cybersecurity event is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state under subsection (1) or (2), a licensee shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

(4) A licensee shall provide any notice required under this section without unreasonable delay. A licensee may delay providing notice without violating this subsection if either of the following is met:

(a) A delay is necessary in order for the licensee to take any measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the database. However, the licensee shall provide the notice required under this subsection without unreasonable delay after the licensee completes the measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the database.

(b) A law enforcement agency determines and advises the licensee that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the licensee shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

(5) A licensee shall provide any notice required under this section by providing 1 or more of the following to the recipient:

(a) Written notice sent to the recipient at the recipient's postal address in the records of the licensee.

(b) Written notice sent electronically to the recipient if any of the following are met:

(i) The recipient has expressly consented to receive electronic notice.

(ii) The licensee has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the licensee reasonably believes that it has the recipient's current electronic mail address.

(iii) The licensee conducts its business primarily through internet account transactions or on the internet.

(c) If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the licensee if all of the following are met:

(i) The notice is not given in whole or in part by use of a recorded message.

(ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the licensee also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the licensee and the recipient within 3 business days after the initial attempt to provide telephonic notice.

(d) Substitute notice, if the licensee demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000.00 or that the licensee has to provide notice to more than 500,000 residents of this state. A licensee provides substitute notice under this subdivision by doing all of the following:

(i) If the licensee has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.

(ii) If the licensee maintains a website, conspicuously posting the notice on that website.

(iii) Notifying major statewide media. A notification under this subparagraph must include a telephone number or

a website address that a person may use to obtain additional assistance and information.

(6) A notice under this section must do all of the following:

(a) For a notice provided under subsection (5)(a) or (b), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g).

(b) For a notice provided under subsection (5)(c), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.

(c) Describe the cybersecurity event in general terms.

(d) Describe the type of personal information that is the subject of the unauthorized access or use.

(e) If applicable, generally describe what the licensee providing the notice has done to protect data from further security breaches.

(f) Include a telephone number where a notice recipient may obtain assistance or additional information.

(g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

(7) A licensee may provide any notice required under this section under an agreement between the licensee and another licensee, if the notice provided under the agreement does not conflict with this section.

(8) Except as provided in this subsection, after a licensee provides a notice under this section, the licensee shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the cybersecurity event without unreasonable delay. A notification under this subsection must include the number of notices that the licensee provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:

(a) The licensee is required under this section to provide notice of a cybersecurity event to 1,000 or fewer residents of this state.

(b) The licensee is subject to 15 USC 6801 to 6809.

(9) A licensee that is subject to and complies with the health insurance portability and accountability act of 1996, Public Law 104-191, and with regulations promulgated under that act, 45 CFR parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice is considered to be in compliance with this section.

(10) A person that provides notice of a cybersecurity event in the manner described in this section when a cybersecurity event has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows:

(a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than $250.00 for each violation, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than $500.00 for each violation, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $750.00 for each violation, or both.

(11) Subject to subsection (12), a person that knowingly fails to provide a notice of a cybersecurity event required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

(12) The aggregate liability of a person for civil fines under subsection (11) for multiple violations of subsection (11) that arise from the same cybersecurity event must not exceed $750,000.00.

(13) Subsections (10) and (11) do not affect the availability of any civil remedy for a violation of state or federal law.

(14) This section applies to the discovery or notification of a breach of the security of a database that occurs after December 31, 2019.

(15) This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.

(16) This section deals with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of this state to regulate, directly or indirectly, any matter expressly set forth in this section is preempted.

(17) As used in this section:

(a) "Data" means computerized information.

(b) "Identity theft" means a person doing any of the following:

(i) With intent to defraud or violate the law, using or attempting to use the personal information of another person to do either of the following:

(A) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(B) Commit another unlawful act.

(ii) By concealing, withholding, or misrepresenting the person's identity, using or attempting to use the personal information of another person to do either of the following:

(A) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(B) Commit another unlawful act.

(c) "Personal information" means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state:

(i) A Social Security number.

(ii) A driver license number or state personal identification card number.

(iii) A demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

History: Add. 2018, Act 690, Eff. Jan. 20, 2021
Popular Name: Act 218