A.R.S. § 18-552

Current through chapter 1 of the 56th Legislature's 2nd Regular session (2024), including all legislation enacted through March 1, 2024

LexisNexis® Arizona Annotated Revised Statutes > Title 18 Information Technology (Chs. 1 — 6) > Chapter 5 Network Security (Arts. 1 — 4) > Article 4. Data Security Breaches (§§ 18-551 — 18-552)

18-552. Notification of security system breaches; requirements; enforcement; confidentiality; civil penalty; preemption; exceptions

A. If a person that conducts business in this state and that owns, maintains or licenses unencrypted and unredacted computerized personal information becomes aware of a security incident, the person shall conduct an investigation to promptly determine whether there has been a security system breach.

B. If the investigation results in a determination that there has been a security system breach, the person that owns or licenses the computerized data, within forty-five days after the determination, shall:

1. Notify the individuals affected pursuant to subsection E of this section and subject to the needs of law enforcement as provided in subsection D of this section.

2. If the breach requires notification of more than one thousand individuals, notify both:

(a) The three largest nationwide consumer reporting agencies.

(b) The attorney general and the director of the Arizona department of homeland security, in writing, in a form prescribed by rule or order of the attorney general or the director of the Arizona department of homeland security or by providing the attorney general or the director of the Arizona department of homeland security with a copy of the notification provided pursuant to paragraph 1 of this subsection. In the absence of a common form developed by the attorney general and the Arizona department of homeland security, nothing shall prohibit a person from submitting the same notification to the attorney general and the Arizona department of homeland security to meet the requirements of this subsection.

C. A person that maintains unencrypted and unredacted computerized personal information that the person does not own or license shall notify, as soon as practicable, the owner or licensee of the information on discovering any security system breach and cooperate with the owner or the licensee of the personal information, including sharing information relevant to the breach with the owner or licensee. The person that maintains the data under an agreement with the owner or licensee is not required to provide the notifications required by subsection B of this section unless the agreement stipulates otherwise.

D. The notifications required by subsection B of this section may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation. On being informed by the law enforcement agency that the notifications no longer compromise the

investigation, the person shall make the required notifications, as applicable, within forty-five days.

E. The notification required by subsection B, paragraph 1 of this section shall include at least the following:

1. The approximate date of the breach.

2. A brief description of the personal information included in the breach.

3. The toll-free numbers and addresses for the three largest nationwide consumer reporting agencies.

4. The toll-free number, address and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters.

F. The notification required by subsection B, paragraph 1 of this section shall be provided by one of the following methods:

1. Written notice.

2. An email notice if the person has email addresses for the individuals who are subject to the notice.

3. Telephonic notice, if telephonic contact is made directly with the affected individuals and is not through a prerecorded message.

4. Substitute notice if the person demonstrates that the cost of providing notice pursuant to paragraph 1, 2 or 3 of this subsection would exceed $50,000, that the affected class of subject individuals to be notified exceeds one hundred thousand individuals or that the person does not have sufficient contact information. Substitute notice consists of all of the following:

(a) A written letter to the attorney general that demonstrates the facts necessary for substitute notice.

(b) Conspicuous posting of the notice for at least forty-five days on the website of the person if the person maintains one.

G. If a breach involves personal information as prescribed in section 18-551, paragraph 7, subdivision (a), item (ii) for an online account and does not involve personal information as defined in section 18-551, paragraph 7, subdivision (a), item (i), the person may comply with this section by providing the notification in an electronic or other form that directs the individual whose personal information has been breached to promptly change the individual's password and security question or answer, as applicable, or to take other steps that are appropriate to protect the online account with the person and all other online accounts for which the individual whose personal information has been breached uses the same user name and email address and password or security question or answer. If the breach of personal information as prescribed in section 18-551, paragraph 7, subdivision (a), item (ii) is for login credentials of an email account furnished by the person, the person is not required to comply with this section by providing the notification to that email address, but may comply with this section by providing notification by another method described in this subsection or by providing clear and conspicuous notification delivered to the individual online when the individual is connected to the online account from an internet protocol address or online location from which the person knows the individual customarily accesses the account. The person satisfies the notification requirement with regard to the individual's account with the person by requiring the individual to reset the individual's password or security question and answer for that account, if the person also notifies the individual to change the same password

or security question and answer for all other online accounts for which the individual uses the same user name or email address and password or security question or answer.

H. A person that maintains the person's own notification procedures as part of an information security policy for the treatment of personal information and that is otherwise consistent with the requirements of this article, including the forty-five-day notification period required by subsection B of this section, is deemed to be in compliance with the notification requirements of subsection B, paragraph 1 of this section if the person notifies subject individuals in accordance with the person's policies if a security system breach occurs.

I. A person that complies with the notification requirements or security system breach procedures pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator is deemed to be in compliance with the requirements of subsection B, paragraph 1 of this section.

J. A person is not required to make the notification required by subsection B of this section if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.

K. Except for notifications provided pursuant to subsection F of this section, notifications provided to the attorney general and the director of the Arizona department of homeland security pursuant to this section are confidential pursuant to section 44-1525 and are exempt from disclosure under title 39.

L. A knowing and wilful violation of this section is an unlawful practice pursuant to section 44-1522, and only the attorney general may enforce such a violation by investigating and taking appropriate action pursuant to title 44, chapter 10, article 7. The attorney general may impose a civil penalty for a violation of this article not to exceed the lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals, but the maximum civil penalty from a breach or series of related breaches may not exceed $500,000. This section does not prevent the attorney general from recovering restitution for affected individuals.

M. The state legislature determines that security system breach notification is a matter of statewide concern. The power to regulate security system breach notification is preempted by this state, and this article supersedes and preempts all municipal and county laws, charters, ordinances and rules relating to issues regulated by this article.

N. This article does not apply to either of the following:

1. A person that is subject to title V of the Gramm-Leach-Bliley act (P.L. 106-102; 113 Stat. 1338; 15 United States Code sections 6801 through 6809).

2. A covered entity or business associates as defined under regulations implementing the health insurance portability and accountability act of 1996, 45 Code of Federal Regulations section 160.103 (2013) or a charitable fundraising foundation or nonprofit corporation whose primary purpose is to support a specified covered entity, if the charitable fundraising foundation or nonprofit corporation complies with any applicable provision of the health insurance portability and accountability act of 1996 and its implementing regulations.

O. The department of public safety, a county sheriff's department, a municipal police department, a prosecution agency and a court shall create and maintain an information security policy that includes notification procedures for a security system breach of the department of public safety, the county sheriff's department, the municipal police department, the prosecuting agency or the court.

History

Laws 2006, Ch. 232, § 1; Laws 2007, Ch. 23, § 1; Laws 2016, 2nd Reg. Sess., Ch. 80, §§ 3(E), 15; 2016 2nd Reg. Sess. Ch. 102, § 1, effective August 6, 2016; renumbered from § 18-545 by 2018 2nd Reg. Sess. Ch. 177, § 2, effective August 3, 2018; 2022 2nd Reg. Sess. Ch. 81, § 1, effective September 24, 2022.

End of Document