

House Engrossed

data security breach; notification

State of Arizona
House of Representatives
Fifty-fifth Legislature
Second Regular Session
2022

CHAPTER 81
HOUSE BILL 2146

AN ACT

AMENDING SECTION 18-552, ARIZONA REVISED STATUTES; RELATING TO DATA SECURITY BREACHES.

(TEXT OF BILL BEGINS ON NEXT PAGE)

1 Be it enacted by the Legislature of the State of Arizona:

2 Section 1. Section 18-552, Arizona Revised Statutes, is amended to
3 read:

4 18-552. Notification of security system breaches;
5 requirements; enforcement; confidentiality; civil
6 penalty; preemption; exceptions

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

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

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

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

20 (a) The three largest nationwide consumer reporting agencies.

21 (b) The attorney general AND THE DIRECTOR OF THE ARIZONA DEPARTMENT
22 OF HOMELAND SECURITY, in writing, in a form prescribed by rule or order of
23 the attorney general OR THE DIRECTOR OF THE ARIZONA DEPARTMENT OF HOMELAND
24 SECURITY or by providing the attorney general OR THE DIRECTOR OF THE
25 ARIZONA DEPARTMENT OF HOMELAND SECURITY with a copy of the notification
26 provided pursuant to paragraph 1 of this subsection. IN THE ABSENCE OF A
27 COMMON FORM DEVELOPED BY THE ATTORNEY GENERAL AND THE ARIZONA DEPARTMENT
28 OF HOMELAND SECURITY, NOTHING SHALL PROHIBIT A PERSON FROM SUBMITTING THE
29 SAME NOTIFICATION TO THE ATTORNEY GENERAL AND THE ARIZONA DEPARTMENT OF
30 HOMELAND SECURITY TO MEET THE REQUIREMENTS OF THIS SUBSECTION.

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

40 D. The notifications required by subsection B of this section may
41 be delayed if a law enforcement agency advises the person that the
42 notifications will impede a criminal investigation. On being informed by
43 the law enforcement agency that the notifications no longer compromise the
44 investigation, the person shall make the required notifications, as
45 applicable, within forty-five days.

1 E. The notification required by subsection B, paragraph 1 of this
2 section shall include at least the following:
3 1. The approximate date of the breach.
4 2. A brief description of the personal information included in the
5 breach.
6 3. The toll-free numbers and addresses for the three largest
7 nationwide consumer reporting agencies.
8 4. The toll-free number, address and website address for the
9 federal trade commission or any federal agency that assists consumers with
10 identity theft matters.
11 F. The notification required by subsection B, paragraph 1 of this
12 section shall be provided by one of the following methods:
13 1. Written notice.
14 2. An ~~e-mail~~ EMAIL notice if the person has ~~e-mail~~ EMAIL addresses
15 for the individuals who are subject to the notice.
16 3. Telephonic notice, if telephonic contact is made directly with
17 the affected individuals and is not through a prerecorded message.
18 4. Substitute notice if the person demonstrates that the cost of
19 providing notice pursuant to paragraph 1, 2 or 3 of this subsection would
20 exceed ~~fifty thousand dollars~~ \$50,000, that the affected class of subject
21 individuals to be notified exceeds one hundred thousand individuals, or
22 that the person does not have sufficient contact information. Substitute
23 notice consists of all of the following:
24 (a) A written letter to the attorney general that demonstrates the
25 facts necessary for substitute notice.
26 (b) Conspicuous posting of the notice for at least forty-five days
27 on the website of the person if the person maintains one.
28 G. If a breach involves personal information as prescribed in
29 section 18-551, paragraph 7, subdivision (a), item (ii) for an online
30 account and does not involve personal information as defined in section
31 18-551, paragraph 7, subdivision (a), item (i), the person may comply with
32 this section by providing the notification in an electronic or other form
33 that directs the individual whose personal information has been breached
34 to promptly change the individual's password and security question or
35 answer, as applicable, or to take other steps that are appropriate to
36 protect the online account with the person and all other online accounts
37 for which the individual whose personal information has been breached uses
38 the same user name and ~~e-mail~~ EMAIL address and password or security
39 question or answer. If the breach of personal information as prescribed
40 in section 18-551, paragraph 7, subdivision (a), item (ii) is for login
41 credentials of an ~~e-mail~~ EMAIL account furnished by the person, the person
42 is not required to comply with this section by providing the notification
43 to that ~~e-mail~~ EMAIL address, but may comply with this section by
44 providing notification by another method described in this subsection or
45 by providing clear and conspicuous notification delivered to the

1 individual online when the individual is connected to the online account
2 from an internet protocol address or online location from which the person
3 knows the individual customarily accesses the account. The person
4 satisfies the notification requirement with regard to the individual's
5 account with the person by requiring the individual to reset the
6 individual's password or security question and answer for that account, if
7 the person also notifies the individual to change the same password or
8 security question and answer for all other online accounts for which the
9 individual uses the same user name or ~~e-mail~~ EMAIL address and password or
10 security question or answer.

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

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

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

30 K. Except for notifications provided pursuant to subsection F of
31 this section, notifications provided to the attorney general **AND THE**
32 **DIRECTOR OF THE ARIZONA DEPARTMENT OF HOMELAND SECURITY** pursuant to this
33 section are confidential pursuant to section 44-1525 and are exempt from
34 disclosure under title 39.

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

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

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

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

10 2. A covered entity or business associates as defined under
11 regulations implementing the health insurance portability and
12 accountability act of 1996, 45 Code of Federal Regulations section 160.103
13 (2013) or a charitable ~~fund-raising~~ FUNDRAISING foundation or nonprofit
14 corporation whose primary purpose is to support a specified covered
15 entity, if the charitable ~~fund-raising~~ FUNDRAISING foundation or nonprofit
16 corporation complies with any applicable provision of the health insurance
17 portability and accountability act of 1996 and its implementing
18 regulations.

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

APPROVED BY THE GOVERNOR MARCH 29, 2022.

FILED IN THE OFFICE OF THE SECRETARY OF STATE MARCH 29, 2022.