Senate Engrossed House Bill

State of Arizona
House of Representatives
Fifty-third Legislature
Second Regular Session
2018

CHAPTER 177

HOUSE BILL 2154

AN ACT

AMENDING TITLE 18, CHAPTER 5, ARIZONA REVISED STATUTES, BY ADDING ARTICLE 4; PROVIDING FOR TRANSFERRING AND RENUMBERING; AMENDING SECTION 18-552, ARIZONA REVISED STATUTES, AS TRANSFERRED AND RENUMBERED; AMENDING SECTIONS 33-1701 AND 36-3802, ARIZONA REVISED STATUTES; REPEALING LAWS 2006, CHAPTER 232, SECTION 3, AS AMENDED BY LAWS 2016, CHAPTER 80, SECTION 31; RELATING TO DATA SECURITY BREACHES.

(TEXT OF BILL BEGINS ON NEXT PAGE)
Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 18, chapter 5, Arizona Revised Statutes, is amended by adding article 4, to read:

ARTICLE 4. DATA SECURITY BREACHES

18-551. Definitions
IN THIS ARTICLE, UNLESS THE CONTEXT OTHERWISE REQUIRES:
1. "BREACH" OR "SECURITY SYSTEM BREACH":
   (a) MEANS AN UNAUTHORIZED ACQUISITION OF AND UNAUTHORIZED ACCESS THAT MATERIALLY COMPROMISES THE SECURITY OR CONFIDENTIALITY OF UNENCRYPTED AND UNREDACTED COMPUTERIZED PERSONAL INFORMATION MAINTAINED AS PART OF A DATABASE OF PERSONAL INFORMATION REGARDING MULTIPLE INDIVIDUALS.
   (b) DOES NOT INCLUDE A GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY A PERSON'S EMPLOYEE OR AGENT FOR THE PURPOSES OF THE PERSON IF THE PERSONAL INFORMATION IS NOT USED FOR A PURPOSE UNRELATED TO THE PERSON AND IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.
3. "ENCRYPT" MEANS TO USE A PROCESS TO TRANSFORM DATA INTO A FORM THAT RENDERS THE DATA UNREADABLE OR UNUSABLE WITHOUT USING A CONFIDENTIAL PROCESS OR KEY.
4. "INDIVIDUAL" MEANS A RESIDENT OF THIS STATE WHO HAS A PRINCIPAL MAILING ADDRESS IN THIS STATE AS REFLECTED IN THE RECORDS OF THE PERSON CONDUCTING BUSINESS IN THIS STATE AT THE TIME OF THE BREACH.
5. "NATIONWIDE CONSUMER REPORTING AGENCY":
   (a) MEANS A CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS AS DEFINED IN 15 UNITED STATES CODE SECTION 1681a(p).
   (b) DOES NOT INCLUDE A NATIONWIDE SPECIALTY CONSUMER REPORTING AGENCY AS DEFINED IN 15 UNITED STATES CODE SECTION 1681a(x).
6. "PERSON":
   (a) MEANS A NATURAL PERSON, CORPORATION, BUSINESS TRUST, ESTATE, TRUST, PARTNERSHIP, ASSOCIATION, JOINT VENTURE, GOVERNMENT OR GOVERNMENTAL SUBDIVISION OR AGENCY OR ANY OTHER LEGAL OR COMMERCIAL ENTITY.
   (b) DOES NOT INCLUDE THE DEPARTMENT OF PUBLIC SAFETY, A COUNTY SHERIFF'S DEPARTMENT, A MUNICIPAL POLICE DEPARTMENT, A PROSECUTION AGENCY OR A COURT.
7. "PERSONAL INFORMATION":
   (a) MEANS ANY OF THE FOLLOWING:
      (i) AN INDIVIDUAL'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION WITH ONE OR MORE SPECIFIED DATA ELEMENTS.
      (ii) AN INDIVIDUAL'S USER NAME OR E-MAIL ADDRESS, IN COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND ANSWER, THAT ALLOWS ACCESS TO AN ONLINE ACCOUNT.
(b) DOES NOT INCLUDE PUBLICLY AVAILABLE INFORMATION THAT IS
LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE OR LOCAL
GOVERNMENT RECORDS OR WIDELY DISTRIBUTED MEDIA.

8. "PROSECUTION AGENCY" MEANS THE ATTORNEY GENERAL, A COUNTY
ATTORNEY OR A MUNICIPAL PROSECUTOR.

9. "REDACT" MEANS TO ALTER OR TRUNCATE A NUMBER SO THAT NOT MORE
THAN THE LAST FOUR DIGITS ARE ACCESSIBLE AND AT LEAST TWO DIGITS HAVE BEEN
REMOVED.

10. "SECURITY INCIDENT" MEANS AN EVENT THAT CREATES REASONABLE
SUSPICION THAT A PERSON'S INFORMATION SYSTEMS OR COMPUTERIZED DATA MAY
HAVE BEEN COMPROMISED OR THAT MEASURES PUT IN PLACE TO PROTECT THE
PERSON'S INFORMATION SYSTEMS OR COMPUTERIZED DATA MAY HAVE FAILED.

11. "SPECIFIED DATA ELEMENT" MEANS ANY OF THE FOLLOWING:
(a) AN INDIVIDUAL'S SOCIAL SECURITY NUMBER.
(b) THE NUMBER ON AN INDIVIDUAL'S DRIVER LICENSE ISSUED PURSUANT TO
SECTION 28-3166 OR NONOPERATING IDENTIFICATION LICENSE ISSUED PURSUANT TO
SECTION 28-3165.
(c) A PRIVATE KEY THAT IS UNIQUE TO AN INDIVIDUAL AND THAT IS USED
TO AUTHENTICATE OR SIGN AN ELECTRONIC RECORD.
(d) AN INDIVIDUAL'S FINANCIAL ACCOUNT NUMBER OR CREDIT OR DEBIT
CARD NUMBER IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE OR
PASSWORD THAT WOULD ALLOW ACCESS TO THE INDIVIDUAL'S FINANCIAL ACCOUNT.
(e) AN INDIVIDUAL'S HEALTH INSURANCE IDENTIFICATION NUMBER.
(f) INFORMATION ABOUT AN INDIVIDUAL'S MEDICAL OR MENTAL HEALTH
TREATMENT OR DIAGNOSIS BY A HEALTH CARE PROFESSIONAL.
(g) AN INDIVIDUAL'S PASSPORT NUMBER.
(h) AN INDIVIDUAL'S TAXPAYER IDENTIFICATION NUMBER OR AN IDENTITY
PROTECTION PERSONAL IDENTIFICATION NUMBER ISSUED BY THE UNITED STATES
INTERNAL REVENUE SERVICE.
(i) UNIQUE BIOMETRIC DATA GENERATED FROM A MEASUREMENT OR ANALYSIS
OF HUMAN BODY CHARACTERISTICS TO AUTHENTICATE AN INDIVIDUAL WHEN THE
INDIVIDUAL ACCESSES AN ONLINE ACCOUNT.

Sec. 2. Section 18-545, Arizona Revised Statutes, is transferred
and renumbered for placement in title 18, chapter 5, article 4, Arizona
Revised Statutes, as section 18-552 and, as so renumbered, is amended to
read:

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

A. When IF a person that conducts business in this state and that
owns, MAINTAINS or licenses unencrypted AND UNREDACTED computerized data
that includes personal information becomes aware of an A SECURITY incident
of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the
person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system.

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

1. Notify the individuals affected. The notice shall be made in the most expedient manner possible and without unreasonable delay pursuant to subsection E of this section and subject to the needs of law enforcement as provided in subsection D of this section and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected or to restore the reasonable integrity of the data system.

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, in writing, in a form prescribed by rule or order of the Attorney General or by providing the Attorney General with a copy of the notification provided pursuant to paragraph 1 of this subsection.

B. C. A person that maintains unencrypted and unredacted computerized data that includes 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 of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include, including sharing information relevant to the breach of the security of the system with the owner or licensee. The person that owns or licenses the computerized data shall provide notice to the individual pursuant to this section. The person that maintains the data under an agreement with the owner or licensee is not required to provide notice to the individual pursuant to this section if the notifications required by subsection B of this section are made by the person that maintains the data under an agreement with the owner or licensee and the agreement stipulates otherwise.

B. D. The notification required by subsection A, 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. Electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the electronic signatures in global and national commerce act (P.L. 106-229, 114 Stat. 464, 15 United States Code section 7001).

2. AN E-MAIL NOTICE IF THE PERSON HAS E-MAIL 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 fifty thousand dollars or, that the affected class of subject individuals to be notified exceeds one hundred thousand persons, or THAT the person does not have sufficient contact information. Substitute notice shall consist of all of the following:

(a) Electronic mail notice if the person has electronic mail addresses for the individuals subject to the notice.

(b) 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.

(c) Notification to major statewide media.

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 E-MAIL 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 E-MAIL ACCOUNT FURNISHED BY THE PERSON, THE PERSON IS NOT REQUIRED
TO COMPLY WITH THIS SECTION BY PROVIDING THE NOTIFICATION TO THAT E-MAIL
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 E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR ANSWER.

E. A person who 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 section shall be deemed to be in compliance with the
FORTY-FIVE-DAY NOTIFICATION PERIOD REQUIRED BY SUBSECTION B OF THIS
SECTION, IS deemed to be in compliance with the notification requirements
of this section if the person notifies subject individuals in accordance with the person's policies if a
breach of the security system occurs.

F. A person that complies with the notification requirements or
security 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.

G. A person is not required to disclose a breach of the
security of the system if the person, or an independent third-party forensic auditor
or a law enforcement agency, after a reasonable investigation, determines
that a breach of the security of the system has not occurred or is not reasonably likely to
occur RESULT IN SUBSTANTIAL ECONOMIC LOSS TO AFFECTED INDIVIDUALS.

H. This section may only be enforced by the attorney general. The
attorney general may bring an action to obtain actual damages for a willful
and knowing violation of this section and a civil penalty not to exceed
ten thousand dollars per breach of the security of the system or series of
breaches of a similar nature that are discovered in a single
investigation.
H.B. 2154

K. EXCEPT FOR NOTIFICATIONS PROVIDED PURSUANT TO SUBSECTION F OF THIS SECTION, NOTIFICATIONS PROVIDED TO THE ATTORNEY GENERAL 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 TEN THOUSAND DOLLARS 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 FIVE HUNDRED THOUSAND DOLLARS. 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 section shall supersede ARTICLE SUPERSEDES and preempt PREEMPTS all municipal and county laws, charters, ordinances and rules relating to issues regulated by this section ARTICLE.

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


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 breach of the security system BREACH of the department of public safety, the county sheriff's department, the municipal police department, the prosecuting agency or the court.

L. For the purposes of this section:

1. "Breach", "breach of the security of the system", "breach of the security system" or "security breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information
maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further wilful unauthorized disclosure.

2. “Court” means the supreme court, court of appeals, superior court, courts inferior to the superior court and justice courts.

3. “Encrypted” means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

4. “Individual” means a person that is a resident of this state as determined by a principal mailing address in this state as reflected in the records of the person conducting business in this state at the time of the breach.

5. “Person” means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency or any other legal or commercial entity. Person does not include the department of public safety, a county sheriff’s department, a municipal police department, a prosecution agency or a court.

6. “Personal information”:
   (a) Means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or unusable:
      (i) The individual’s social security number.
      (ii) The individual’s number on a driver license issued pursuant to section 28-3166 or number on a nonoperating identification license issued pursuant to section 28-3165.
      (iii) The individual’s financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual’s financial account.
   (b) Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

7. “Prosecution agency” means the attorney general, any county attorney or any municipal prosecutor.

8. “Redact” means alter or truncate data such that no more than the last four digits of a social security number, driver license number, nonoperating identification license number, financial account number or credit or debit card number is accessible as part of the personal information.
Sec. 3. Section 33-1701, Arizona Revised Statutes, is amended to read:

33-1701. Definitions; exception

A. In this article, unless the context otherwise requires:

1. "Default" means the failure to perform on time any obligation or duty set forth in the rental agreement.

2. "Department" means the Arizona game and fish department in the case of motorized watercraft and the department of transportation in the case of all other vehicles.

3. "Electronic mail" means an electronic message or an executable program or computer file that contains an image of a message that is transmitted between two or more computers or electronic terminals and includes electronic messages that are transmitted within or between computer networks from which a confirmation of receipt is received.

4. "Last known address" means that postal address or electronic address provided by the occupant in the rental agreement or the postal address or electronic address provided by the occupant in a subsequent written notice of a change of address.

5. "Late fee" means a reasonable fee or charge that is assessed by the operator for the failure of the occupant to pay rent when due pursuant to section 33-1703, subsection D.

6. "Leased space" means the storage space or spaces at the self-service storage facility that are rented to an occupant pursuant to a rental agreement.

7. "Net proceeds" means the total proceeds received from the lien sale less the total amount of the lien.

8. "Occupant" means a person or the person's sublessee, successor or assign, entitled to the use of the leased space at a self-service storage facility under a rental agreement, to the exclusion of others.

9. "Operator" means the owner, operator, lessor or sublessor of a self-service storage facility, an agent or any other person authorized to manage the facility.

10. "Personal information" has the same meaning prescribed in section 18-545 and includes passport information and medical or legal records.

11. "Personal property" means movable property that is not affixed to land and includes but is not limited to goods, wares, merchandise, household items and furnishings and vehicles.

12. "Protected property" means personal property for which the sale or disposal of which is regulated by state or federal law and that is one of the following:

(a) Documents, files or electronic data that contains personal information relating to clients, customers, patients or others in connection with the occupant's business.
(b) Alcoholic beverages.
(c) Pharmaceuticals other than those dispensed by a licensed pharmacy for the occupant's personal use.
(d) Firearms.

13. "Registered owner" means an owner of a vehicle as stated in the official records of the department.

14. "Rental agreement" means any written agreement provided to the occupant that establishes or modifies the terms, conditions or rules concerning the use and occupancy of leased space at a self-service storage facility.

15. "Self-service storage facility" means any real property used for renting or leasing storage spaces in which the occupants themselves customarily store and remove their own personal property on a self-service basis.

16. "Vehicle" means a motor vehicle, a trailer or a semitrailer as defined in section 28-101 and a motorized watercraft as defined in section 5-301.

17. "Verified mail" means any method of mailing that is offered by the United States postal service and that provides evidence of mailing.

B. This article does not apply to a warehouseman unless the warehouseman issues a warehouse receipt, bill of lading or other document of title for the personal property stored.

Sec. 4. Section 36-3802, Arizona Revised Statutes, is amended to read:

36-3802. Individual rights
A. A health information organization must provide the following rights to individuals:

1. To opt out of participating in the health information organization pursuant to section 36-3803.

2. To request a copy of the individual's individually identifiable health information that is available through the health information organization. The health information organization may provide this right directly or may require health care providers participating in the health information organization to provide access to individuals. The copy may be provided electronically, if the individual requesting the copy consents to electronic delivery of the individually identifiable health information, and must be provided to the individual within thirty days after the individual's request. Charges for copies are governed by section 12-2295.

3. To request THE amendment of incorrect individually identifiable health information available through the health information organization.

4. To request a list of the persons who have accessed the individual's individually identifiable health information through the health information organization for a period of at least three years.
before the individual's request. This list must be provided to the
individual within thirty days after the individual's request.

5. To be notified, pursuant to section 10-545 18-552 and 45 Code of
Federal Regulations part 164, subpart D, of a breach at the health
information organization that affects the individual's individually
identifiable health information.

B. If an individual does not have the capacity to make health care
decisions, the individual's health care decision maker may exercise all
individual rights in this chapter on behalf of the individual.

Sec. 5. Repeal

Laws 2006, chapter 232, section 3, as amended by Laws 2016, chapter
80, section 31, is repealed.

APPROVED BY THE GOVERNOR APRIL 11, 2018.