2016 Ariz. HB 2363

Enacted, April 5, 2016

Reporter
2016 Ariz. ALS 102; 2016 Ariz. Sess. Laws 102; 2016 Ariz. Ch. 102; 2016 Ariz. HB 2363

ARIZONA ADVANCE LEGISLATIVE SERVICE > ARIZONA 52ND LEGISLATURE - SECOND REGULAR SESSION > CHAPTER 102 > HOUSE BILL 2363

Notice

Added: Text highlighted in green
Deleted: ~~Red text with a strikethrough~~

Synopsis

AMENDING *SECTIONS 44-7501* AND *44-7601, ARIZONA REVISED STATUTES*; RELATING TO SECURITY OF PERSONAL INFORMATION.

Text

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

Section 1. Section *44-7501*, Arizona Revised Statutes, is amended to read:

44-7501. Notification of breach of security system; enforcement; civil penalty; preemption; exceptions; definitions

A. When a person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an 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. If the investigation results in a determination that there has been a breach in the security system, the person shall notify the individuals affected. The notice shall be made in the most expedient manner possible and without unreasonable delay subject to the needs of law enforcement as provided in subsection C 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.

B. A person that maintains unencrypted computerized data that includes personal information that the person does not own shall notify and cooperate with the owner or the licensee of the information of any breach of the security of the system following discovery of the breach without unreasonable delay. Cooperation shall include 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 maintained the data under an agreement with the owner or licensee is not required to provide notice to the individual pursuant to this section unless the agreement stipulates otherwise.

C. The notification required by subsection A of this section may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. The person shall make the notification after the law enforcement agency determines that it will not compromise the investigation.

D. The disclosure required by subsection A 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).

3. Telephonic notice.

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 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) Conspicuous posting of the notice on the web site of the person if the person maintains one.

(c) Notification to major statewide media.

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 WHO is otherwise consistent with the requirements of this section shall be 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 this section.

G. A person is not required to disclose a breach of the security of the system if the person 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.

H. This section may only be enforced by the attorney general. The attorney general may bring an action to obtain actual damages for a wilful 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.

I. The state legislature determines that security system breach notification is a matter of statewide concern. The power to regulate security breach notification is preempted by this state and this section shall supersede and preempt all municipal and county laws, charters, ordinances and rules relating to issues regulated by this chapter.

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

1. A person subject to title V of the Gramm-Leach-Bliley act ~~of 1999~~ (*P.L. 106-102*; *113 Stat. 1338*; 15 United States Code sections 6801 through 6809).

2. Covered entities AND BUSINESS ASSOCIATES as defined under regulations implementing the health insurance portability and accountability act, *45 Code of Federal Regulations section 160.103* ~~(1996)~~(2003).

K. 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 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. 2. Section *44-7601*, Arizona Revised Statutes, is amended to read:

44-7601. Discarding and disposing of records containing personal identifying information; civil penalty; enforcement; definition

A. An entity shall not knowingly discard or dispose of records or documents without redacting the information or destroying the records or documents if the records or documents contain an individual's first and last name or first initial and last name in combination with a corresponding complete:

1. Social security number.

2. Credit card, charge card or debit card number.

3. Retirement account number.

4. Savings, checking or securities entitlement account number.

5. Driver license number or nonoperating identification license number.

B. This section may be enforced by either of the following:

1. A county attorney in the county in which the records or documents were wrongfully discarded or disposed. If a violation occurs by the same entity in multiple counties, a county attorney in a county in which records or documents were ~~not properly~~IMPROPERLY discarded or disposed of, after filing a notice of intent to enforce this section, may send a copy of the notice to the county attorney in each county in which records or documents were not properly discarded or disposed of and may request that the actions be consolidated.

2. The attorney general.

C. A civil penalty shall be imposed for each violation of subsection A OF THIS SECTION arising out of one incident. The civil penalty shall not exceed:

1. Five hundred dollars for a first violation.

2. One thousand dollars for a second violation.

3. Five thousand dollars for a third or subsequent violation.

D. An entity that maintains and complies with the entity's own procedures for the discarding or disposing of records or documents containing the information listed in subsection A OF THIS SECTION that is consistent with the requirements of this section shall be deemed to be in compliance with this section.

E. This section does not apply to any of the following:

1. An entity subject to title V of the Gramm-Leach-Bliley act ~~of 1999~~ (*P.L. 106-102*; *113 Stat. 1338*; 15 United States Code sections 6801 through 6809).

2. Covered entities AND BUSINESS ASSOCIATES as defined under regulations implementing the health insurance portability and accountability act, *45 Code of Federal Regulations section 160.103* ~~(1996)~~(2003).

3. An entity subject to the federal fair credit reporting act~~,~~ (15 United States Code section 1681x).

F. This section only applies to paper records and paper documents.

G. For the purposes of this section, "entity" includes a corporation, foreign corporation, not for profit corporation, profit and not for profit unincorporated association, nonprofit corporation, sole proprietorship, close corporation, corporation sole or limited liability company, a professional corporation, association or limited liability company, a business trust, estate, partnership, registered limited liability partnership, trust or joint venture, A government, governmental subdivision or agency or any other legal or commercial entity.

History

Approved by the Governor April 5, 2016

Effective date: 91st day after adjournment

Sponsor

Carter

End of Document