A.C.A. § 4-110-105

Current through all legislation of the 2023 Regular Session and the 2023 First Extraordinary Session.

AR - Arkansas Code Annotated* > *Title 4 Business and Commercial Law* > *Subtitle 7. Consumer Protection* > *Chapter 110 Personal Information Protection Act

4-110-105. Disclosure of security breaches.

(a)

(1) Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(2) The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(b)

(1) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee that there has been a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(2) If a breach of the security of a system affects the personal information of more than one thousand (1,000) individuals, the person or business required to make a disclosure of the security breach under subdivision (b)(1) of this section shall, at the same time the security breach is disclosed to an affected individual or within forty-five (45) days after the person or business determines that there is a reasonable likelihood of harm to customers, whichever occurs first, disclose the security breach to the Attorney General.

(c)

(1) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

(2) The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.

(e) For purposes of this section, notice may be provided by one (1) of the following methods:

(1) Written notice;

(2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or

(3)

(A) Substitute notice if the person or business demonstrates that:

(i) The cost of providing notice would exceed two hundred fifty thousand dollars ($250,000);

(ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or

(iii) The person or business does not have sufficient contact information.

(B) Substitute notice shall consist of all of the following:

(i) Electronic mail notice when the person or business has an electronic mail address for the subject persons;

(ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and

(iii) Notification by statewide media.

(f) Notwithstanding subsection (e) of this section, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security of the system.

(g)

(1) A person or business shall retain a copy of the written determination of a breach of the security of the system and supporting documentation for five (5) years from the date of determination of the breach of the security of the system.

(2) If the Attorney General submits a written request for the written determination of the breach of the security of the system, the person or business shall send a copy of the written determination of the breach of the security of the system and supporting documentation to the Attorney General no later than thirty (30) days after the date of receipt of the request.

(3) The determination and documentation retained under this subsection are confidential and not subject to public disclosure.

History

Acts 2005, No. 1526, § 1; 2019, No. 1030, §§ 2, 3.

End of Document