

Stricken language would be deleted from and underlined language would be added to the law as it existed prior to this session of the General Assembly.

Act 1526 of the Regular Session

1 State of Arkansas
2 85th General Assembly
3 Regular Session, 2005
4

As Engrossed: S3/18/05

A Bill

SENATE BILL 1167

5 By: Senator Capps
6 By: Representative Schulte
7

8
9 **For An Act To Be Entitled**

10 AN ACT TO PROVIDE NOTICE TO CONSUMERS OF THE
11 DISCLOSURE OF THEIR PERSONAL INFORMATION; AND FOR
12 OTHER PURPOSES.
13

14 **Subtitle**

15 AN ACT TO PROVIDE NOTICE TO CONSUMERS OF
16 THE DISCLOSURE OF THEIR PERSONAL
17 INFORMATION.
18

19
20 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:
21

22 SECTION 1. Arkansas Code Title 4 is amended to add an additional
23 chapter and subchapter to read as follows:
24

25 Chapter 110 – INFORMATION TECHNOLOGY

26 Subchapter 1 – Personal Information Protection

27 4-110-101. Short title.

28 This subchapter shall be known and cited as the "Personal Information
29 Protection Act".
30

31 4-110-102. Findings and purpose.

32 It is the intent of the General Assembly to ensure that sensitive
33 personal information about Arkansas residents is protected. To that end, the
34 purpose of this subchapter is to encourage individuals, businesses, and state
35 agencies that acquire, own, or license personal information about the



1 citizens of the State of Arkansas to provide reasonable security for the
2 information.

3
4 4-110-103. Definitions.

5 As used in this subchapter:

6 (1)(A) "Breach of the security of the system" means unauthorized
7 acquisition of computerized data that compromises the security,
8 confidentiality, or integrity of personal information maintained by a person
9 or business.

10 (B) "Breach of the security of the system" does not
11 include the good faith acquisition of personal information by an employee or
12 agent of the person or business for the legitimate purposes of the person or
13 business if the personal information is not otherwise used or subject to
14 further unauthorized disclosure;

15 (2)(A) "Business" means a sole proprietorship, partnership,
16 corporation, association, or other group, however organized and whether or
17 not organized to operate at a profit, including a financial institution
18 organized, chartered, or holding a license or authorization certificate under
19 the law of this state, any other state, the United States, or of any other
20 country, or the parent or the subsidiary of a financial institution.

21 (B) "Business" includes:

22 (i) An entity that destroys records; and

23 (ii) A state agency;

24 (3) "Customer" means an individual who provides personal
25 information to a business for the purpose of purchasing or leasing a product
26 or obtaining a service from the business;

27 (4) "Individual" means a natural person;

28 (5) "Medical information" means any individually identifiable
29 information, in electronic or physical form, regarding the individual's
30 medical history or medical treatment or diagnosis by a health care
31 professional;

32 (6) "Owns or licenses" includes, but is not limited to, personal
33 information that a business retains as part of the business' internal
34 customer account or for the purpose of using the information in transactions
35 with the person to whom the information relates;

36 (7) "Personal information" means an individual's first name or

1 first initial and his or her last name in combination with any one (1) or
2 more of the following data elements, when either the name or the data element
3 is not encrypted or redacted:

4 (A) Social security number;

5 (B) Driver's license number or Arkansas identification
6 card number;

7 (C) Account number, credit card number, or debit card
8 number in combination with any required security code, access code, or
9 password that would permit access to an individual's financial account; and

10 (D) Medical information;

11 (8)(A) "Records" means any material that contains sensitive
12 personal information in electronic form.

13 (B) "Records" does not include any publicly available
14 directories containing information an individual has voluntarily consented to
15 have publicly disseminated or listed, such as name, address, or telephone
16 number; and

17 (9) "State agencies" or "state agency" means any agency,
18 institution, authority, department, board, commission, bureau, council, or
19 other agency of the State of Arkansas supported by cash funds or the
20 appropriation of state or federal funds.

21
22 4-110-104. Protection of personal information.

23 (a) A person or business shall take all reasonable steps to destroy or
24 arrange for the destruction of a customer's records within its custody or
25 control containing personal information which is no longer to be retained by
26 the person or business by shredding, erasing, or otherwise modifying the
27 personal information in the records to make it unreadable or undecipherable
28 through any means.

29 (b) A person or business that acquires, owns, or licenses personal
30 information about an Arkansas resident shall implement and maintain
31 reasonable security procedures and practices appropriate to the nature of the
32 information to protect the personal information from unauthorized access,
33 destruction, use, modification, or disclosure.

34
35 4-110-105. Disclosure of security breaches.

36 (a)(1) Any person or business that acquires, owns or licenses

1 computerized data that includes personal information shall disclose any
2 breach of the security of the system following discovery or notification of
3 the breach of the security of the system to any resident of Arkansas whose
4 unencrypted personal information was, or is reasonably believed to have been,
5 acquired by an unauthorized person.

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

11 (b) Any person or business that maintains computerized data that
12 includes personal information that the person or business does not own shall
13 notify the owner or licensee of the information of any breach of the security
14 of the system immediately following discovery if the personal information
15 was, or is reasonably believed to have been, acquired by an unauthorized
16 person.

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

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

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

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

28 (1) Written notice;

29 (2) Electronic mail notice, if the notice provided is consistent
30 with the provisions regarding electronic records and signatures set forth in
31 15 U.S.C. § 7001, as it existed on January 1, 2005; or

32 (3)(A) Substitute notice, if the person or business demonstrates
33 that:

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

36 (ii) The affected class of persons to be notified

1 exceeds five hundred thousand (500,000); or

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

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

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

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

10 (iii) Notification by statewide media.

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

18
19 4-110-106. Exemptions.

20 (a)(1) The provisions of this subchapter do not apply to a person or
21 business that is regulated by a state or federal law that provides greater
22 protection to personal information and at least as thorough disclosure
23 requirements for breaches of the security of personal information than that
24 provided by this subchapter.

25 (2) Compliance with the state or federal law shall be deemed
26 compliance with this subchapter with regard to the subjects covered by this
27 subchapter.

28 (b) This section does not relieve a person or business from a duty to
29 comply with any other requirements of other state and federal law regarding
30 the protection and privacy of personal information.

31
32 4-110-107. Waiver.

33 Any waiver of a provision of this subchapter is contrary to public
34 policy, void, and unenforceable.

35
36 4-109-108. Penalties.

1