

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.

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

For An Act To Be Entitled

8
9
10 AN ACT TO PROVIDE NOTICE TO CONSUMERS OF THE
11 DISCLOSURE OF THEIR PERSONAL INFORMATION; AND FOR
12 OTHER PURPOSES.
13

Subtitle

14
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
36 citizens of the State of Arkansas to provide reasonable security for the



1 information.

2
3 4-110-103. Definitions.

4 As used in this subchapter:

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

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

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

20 (B) "Business" includes:

21 (i) An entity that destroys records; and

22 (ii) A state agency;

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

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

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

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

35 (7) "Personal information" means an individual's first name or
36 first initial and his or her last name in combination with any one (1) or

1 more of the following data elements, when either the name or the data element
2 is not encrypted or redacted:

3 (A) Social security number;

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

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

9 (D) Medical information;

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

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

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

20
21 4-110-104. Protection of personal information.

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

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

33
34 4-110-105. Disclosure of security breaches.

35 (a)(1) Any person or business that acquires, owns or licenses
36 computerized data that includes personal information shall disclose any

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

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

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

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

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

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

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

27 (1) Written notice;

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

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

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

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

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

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

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

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

9 (iii) Notification by statewide media.

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

17
18 4-110-106. Exemptions.

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

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

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

30
31 4-110-107. Waiver.

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

34
35 4-109-108. Penalties.

36 Any violation of this subchapter is punishable by action of the

1 Attorney General under the provisions of §§ 4-88-101 through 4-88-115.

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36

/s/ Capps