

THE HOUSE OF REPRESENTATIVES
Wednesday, March 5, 2008

Committee Substitute for
House Bill No. 2245

COMMITTEE SUBSTITUTE FOR HOUSE BILL NO. 2245 - By: INGMIRE of the House and BASS of the Senate.

An Act relating to identity theft; creating short title; defining terms; requiring disclosure of security breach to certain persons without unreasonable delay; providing guidelines for notice requirements; providing enforcement authority to the Attorney General or district attorney; stating enforcement authority for certain financial institutions; stating when discovery and notification procedures of security breaches shall be applied; providing for codification; and providing an effective date.

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

1 SECTION 1. NEW LAW A new section of law to be codified in the Oklahoma
2 Statutes as Section 161 of Title 24, unless there is created a duplication in numbering,
3 reads as follows:

4 This act shall be known and may be cited as the “Security Breach Notification Act”.

5 SECTION 2. NEW LAW A new section of law to be codified in the Oklahoma
6 Statutes as Section 162 of Title 24, unless there is created a duplication in numbering,
7 reads as follows:

8 As used in the Security Breach Notification Act:

9 1. “Breach of the security of a system” means the unauthorized access and
10 acquisition of unencrypted and unredacted computerized data that compromises the

1 security or confidentiality of personal information maintained by an individual or entity
2 as part of a database of personal information regarding multiple individuals and that
3 causes, or the individual or entity reasonably believes has caused or will cause, identity
4 theft or other fraud to any resident of this state. Good faith acquisition of personal
5 information by an employee or agent of an individual or entity for the purposes of the
6 individual or the entity is not a breach of the security of the system, provided that the
7 personal information is not used for a purpose other than a lawful purpose of the
8 individual or entity or subject to further unauthorized disclosure;

9 2. "Entity" includes corporations, business trusts, estates, partnerships, limited
10 partnerships, limited liability partnerships, limited liability companies, associations,
11 organizations, joint ventures, governments, governmental subdivisions, agencies, or
12 instrumentalities, or any other legal entity, whether for profit or not-for-profit;

13 3. "Encrypted" means transformation of data through the use of an algorithmic
14 process into a form in which there is a low probability of assigning meaning without use
15 of a confidential process or key, or securing the information by another method that
16 renders the data elements unreadable or unusable;

17 4. "Financial institution" means any institution the business of which is engaging
18 in financial activities as defined by 15 U.S.C., Section 6809;

19 5. "Individual" means a natural person;

20 6. "Personal information" means the first name or first initial and last name in
21 combination with and linked to any one or more of the following data elements that

1 relate to a resident of this state, when the data elements are neither encrypted nor
2 redacted:

- 3 a. social security number,
- 4 b. driver license number or state identification card number issued in lieu
5 of a driver license, or
- 6 c. financial account number, or credit card or debit card number, in
7 combination with any required security code, access code, or password
8 that would permit access to the financial accounts of a resident.

9 The term does not include information that is lawfully obtained from publicly available
10 information, or from federal, state or local government records lawfully made available to
11 the general public;

12 7. "Notice" means:

- 13 a. written notice to the postal address in the records
14 of the individual or entity,
- 15 b. telephone notice,
- 16 c. electronic notice, or
- 17 d. substitute notice, if the individual or the entity required to provide
18 notice demonstrates that the cost of providing notice will exceed Fifty
19 Thousand Dollars (\$50,000.00), or that the affected class of residents to
20 be notified exceeds 100,000 persons, or that the individual or the entity
21 does not have sufficient contact information or consent to provide

1 notice as described in subparagraph a, b or c of this paragraph.

2 Substitute notice consists of any two of the following:

- 3 (1) e-mail notice if the individual or the entity has e-mail addresses
- 4 for the members of the affected class of residents,
- 5 (2) conspicuous posting of the notice on the Internet web site of the
- 6 individual or the entity if the individual or the entity maintains
- 7 a public Internet web site, or
- 8 (3) notice to major statewide media; and

9 8. "Redact" means alteration or truncation of data such that no more than the
10 following are accessible as part of the personal information:

- 11 a. five digits of a social security number, or
- 12 b. the last four digits of a driver license number, state identification card
- 13 number or account number.

14 SECTION 3. NEW LAW A new section of law to be codified in the Oklahoma
15 Statutes as Section 163 of Title 24, unless there is created a duplication in numbering,
16 reads as follows:

17 A. An individual or entity that owns or licenses computerized data that includes
18 personal information shall disclose any breach of the security of the system following
19 discovery or notification of the breach of the security of the system to any resident of this
20 state whose unencrypted and unredacted personal information was or is reasonably
21 believed to have been accessed and acquired by an unauthorized person and that causes,
22 or the individual or entity reasonably believes has caused or will cause, identity theft or

1 other fraud to any resident of this state. Except as provided in subsection D of this
2 section or in order to take any measures necessary to determine the scope of the breach
3 and to restore the reasonable integrity of the system, the disclosure shall be made
4 without unreasonable delay.

5 B. An individual or entity must disclose the breach of the security of the system if
6 encrypted information is accessed and acquired in an unencrypted form or if the security
7 breach involves a person with access to the encryption key and the individual or entity
8 reasonably believes that such breach has caused or will cause identity theft or other
9 fraud to any resident of this state.

10 C. An individual or entity that maintains computerized data that includes personal
11 information that the individual or entity does not own or license shall notify the owner or
12 licensee of the information of any breach of the security of the system as soon as
13 practicable following discovery, if the personal information was or if the entity
14 reasonably believes was accessed and acquired by an unauthorized person.

15 D. Notice required by this section may be delayed if a law enforcement agency
16 determines and advises the individual or entity that the notice will impede a criminal or
17 civil investigation or homeland or national security. Notice required by this section must
18 be made without unreasonable delay after the law enforcement agency determines that
19 notification will no longer impede the investigation or jeopardize national or homeland
20 security.

1 SECTION 4. NEW LAW A new section of law to be codified in the Oklahoma
2 Statutes as Section 164 of Title 24, unless there is created a duplication in numbering,
3 reads as follows:

4 A. An entity that maintains its own notification procedures as part of an
5 information privacy or security policy for the treatment of personal information and that
6 are consistent with the timing requirements of this act shall be deemed to be in
7 compliance with the notification requirements of this act if it notifies residents of this
8 state in accordance with its procedures in the event of a breach of security of the system.

9 B. 1. A financial institution that complies with the notification requirements
10 prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized
11 Access to Customer Information and Customer Notice is deemed to be in compliance with
12 the provisions of this act.

13 2. An entity that complies with the notification requirements or procedures
14 pursuant to the rules, regulation, procedures, or guidelines established by the primary or
15 functional Federal regulator of the entity shall be deemed to be in compliance with the
16 provisions of this act.

17 SECTION 5. NEW LAW A new section of law to be codified in the Oklahoma
18 Statutes as Section 165 of Title 24, unless there is created a duplication in numbering,
19 reads as follows:

20 A. A violation of this act that results in injury or loss to residents of this state may
21 be enforced by the Attorney General or a district attorney in the same manner as an
22 unlawful practice under the Oklahoma Consumer Protection Act.

1 B. Except as provided in subsection C of this section, the Attorney General or a
2 district attorney shall have exclusive authority to bring action and may obtain either
3 actual damages for a violation of this act or a civil penalty not to exceed One Hundred
4 Fifty Thousand Dollars (\$150,000.00) per breach of the security of the system or series of
5 breaches of a similar nature that are discovered in a single investigation.

6 C. A violation of this act by a state-chartered or state-licensed financial institution
7 shall be enforceable exclusively by the primary state regulator of the financial
8 institution.

9 SECTION 6. NEW LAW A new section of law to be codified in the Oklahoma
10 Statutes as Section 166 of Title 24, unless there is created a duplication in numbering,
11 reads as follows:

12 This act shall apply to the discovery or notification of a breach of the security of the
13 system that occurs on or after November 1, 2008.

14 SECTION 2. This act shall become effective November 1, 2008.

15 COMMITTEE REPORT BY: COMMITTEE ON ECONOMIC DEVELOPMENT AND
16 FINANCIAL SERVICES, dated 03-04-08 - DO PASS, As Amended and Coauthored.

UNDERLINED language denotes Amendments to present Statutes.
BOLD FACE CAPITALIZED language denotes Committee Amendments.
~~Strike thru~~ language denotes deletion from present Statutes.