Okla. Stat. §§ 24-161 to -166

§24-161. Short title.

This act shall be known and may be cited as the "Security Breach Notification Act".

Added by Laws 2008, c. 86, § 1, eff. Nov. 1, 2008.

§24-162. Definitions.

As used in the Security Breach Notification Act:

1. "Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure;

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

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

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

5. "Individual" means a natural person;

6. "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted:

   a. social security number,
   b. driver license number or state identification card number issued in lieu of a driver license, or
   c. financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit

access to the financial accounts of a resident. The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public;

7. "Notice" means:

a. written notice to the postal address in the records of the individual or entity,

b. telephone notice,

c. electronic notice, or

d. substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed Fifty Thousand Dollars ($50,000.00), or that the affected class of residents to be notified exceeds one hundred thousand (100,000) persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in subparagraph a, b or c of this paragraph. Substitute notice consists of any two of the following:

(1) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents,

(2) conspicuous posting of the notice on the Internet web site of the individual or the entity if the individual or the entity maintains a public Internet web site, or

(3) notice to major statewide media; and

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

a. five digits of a social security number, or

b. the last four digits of a driver license number, state identification card number or account number.

Added by Laws 2008, c. 86, § 2, eff. Nov. 1, 2008.

§24-163. Duty to disclose breach.

A. An individual or entity that 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 this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. Except as provided in subsection D of this section or in order to take any measures necessary to determine the scope of the breach and to restore the

reasonable integrity of the system, the disclosure shall be made without unreasonable delay.

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

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

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

Added by Laws 2008, c. 86, § 3, eff. Nov. 1, 2008.

§24-164. Notice procedures deemed in compliance.

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

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

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

Added by Laws 2008, c. 86, § 4, eff. Nov. 1, 2008.

§24-165. Enforcement – Civil penalty limitation.

A. A violation of this act that results in injury or loss to residents of this state may be enforced by the Attorney General or a

district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act.

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

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

Added by Laws 2008, c. 86, § 5, eff. Nov. 1, 2008.

§24-166. Application of act.

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

Added by Laws 2008, c. 86, § 6, eff. Nov. 1, 2008.

Okla. Stat. § 74-3113.1

§74-3113.1. Disclosure of breach of security of computerized personal information.

A. Any state agency, board, commission or other unit or subdivision of state government that 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 in the security of the data to any resident of Oklahoma whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time 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 restore the reasonable integrity of the data system.

B. Any state agency, board, commission or other unit or subdivision of state government that maintains computerized data that includes personal information that the state agency, board, commission or other unit or subdivision of state government does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

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

D. As used in this section:

1. "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the state agency, board, commission or other unit or subdivision of state government. Good faith acquisition of personal information by an employee or agent of the state agency, board, commission or other unit or subdivision of state government for the purposes of that entity shall not be a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;

2. "Personal information" means the first name or first initial and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

a. social security number,

b. driver license number, or

c. account number, credit or debit card number, in

combination with any required security code, access code, or password that would permit access to the financial account of an individual.

Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local public records; and

3. "Notice" means one of the following methods:

a. written notice,

b. electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code, and

c. substitute notice, if the agency demonstrates that the cost of providing notice would exceed Two Hundred Fifty Thousand Dollars ($250,000.00), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when the agency has an e-mail address for the subject persons,

(2) conspicuous posting of the notice on the agency's web site page, if the agency maintains one, and

(3) notification to major statewide media.

E. Notwithstanding paragraph 3 of subsection D of this section, a state agency, board, commission or other unit or subdivision of state government 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 it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Added by Laws 2006, c. 298, § 1, emerg. eff. June 8, 2006.