STATE OF OKLAHOMA

2nd Session of the 59th Legislature (2024)

SENATE BILL 1337 By: Howard

AS INTRODUCED

An Act relating to the Security Breach Notification Act; amending 24 O.S. 2021, Sections 162, 163, 164, 165, and 166, which relate to definitions, duty to disclose breach, notice, enforcement, and application; modifying definitions; requiring notice of security breach of certain information; requiring notice to Attorney General under certain circumstances; specifying contents of required notice; providing exemptions from certain notice requirements; requiring confidentiality of certain information submitted to Attorney General; authorizing Attorney General to promulgate rules; clarifying compliance with certain notice requirements; modifying authorized civil penalties for certain violations; providing exemptions from certain liability; limiting liability for violations under certain circumstances; modifying applicability of act; and providing an effective date.

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

SECTION 1. AMENDATORY 24 O.S. 2021, Section 162, is amended to read as follows:

Section 162. 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 or restricted 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. "Reasonable safeguards" means data protection methods that are appropriate to the nature and volume of the personal information and restricted information. For the purposes of this act, methods shall be deemed reasonable if:

a. such methods are in compliance with applicable federal regulations, or

b. the entity can show by clear and convincing evidence that such methods follow standard business practices for data protection in the relevant industry;

9. "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; and

10. "Restricted information" means any non-personal information about an individual, that alone or in combination with other information including personal information, can be used to distinguish or trace the identity of the individual or that is linked or linkable to the individual, if such information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

SECTION 2. AMENDATORY 24 O.S. 2021, Section 163, is amended to read as follows:

Section 163. A. An individual or entity that owns or licenses computerized data that includes personal information or restricted information shall ~~disclose~~ provide notice of 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~~ shall provide notice of 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 or restricted information that the individual or entity does not own or license shall ~~notify~~ provide notice to 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.

E. 1. An individual or entity required to provide notice in accordance with subsections A, B, or C of this section shall also provide notice to the Attorney General of such breach without unreasonable delay but in no event more than sixty (60) days after discovery of the breach. The notice shall include the date of the breach, the date of its discovery, the nature of the breach, the type of personal information or restricted information exposed, the number of individuals affected, and the estimated monetary impact of the breach to the extent such impact can be determined.

2. A breach of a security system where fewer than two hundred fifty (250) persons are affected within a single breach shall be exempt from the notice requirements of paragraph 1 of this subsection.

3. A breach of a security system maintained by a credit bureau where less than one thousand (1,000) persons are affected within a

single breach shall be exempt from the notice requirements of paragraph 1 of this subsection.

F. Any personal or restricted information submitted to the Attorney General shall be kept confidential pursuant to Section 24A.12 of Title 51 of the Oklahoma Statutes.

G. The Attorney General may promulgate rules as necessary to effectuate the provisions of this section.

SECTION 3. AMENDATORY 24 O.S. 2021, Section 164, is amended to read as follows:

~~Section 164.~~ A. An individual or 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~~ subsection A, B, or C of Section 163 of this title if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.

B. The following entities shall be deemed to be in compliance with the notification requirements of subsection A, B, or C of Section 163 of this title if such entities provide the notice to the Attorney General as required by subsection E of Section 163 of this title:

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. A hospital that complies with the notification requirements prescribed by the Oklahoma Hospital Cybersecurity Protection Act of 2023 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and

3. 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~~.

SECTION 4. AMENDATORY 24 O.S. 2021, Section 165, is amended to read as follows:

Section 165. 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 an action and may obtain ~~either~~ actual damages for a violation of this act ~~or~~ and 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 or Two Thousand Dollars ($2,000.00) per individual per breach, whichever is greater, or a combination of such actual damages and civil penalty. Civil penalties shall be based upon the magnitude of the breach, the extent to which the behavior of the individual or entity contributed to the breach, and any failure to provide the notice required by Section 163 of this title.

C. 1. An individual or entity that uses reasonable safeguards and provides notice as required by Section 163 of this title shall not be subject to civil penalties under this act.

2. An individual or entity that fails to use reasonable safeguards but provides notice as required by Section 163 of this title shall not be subject to the civil penalty set forth in subsection B of this section. Such individuals or entities shall be subject to a civil penalty of One Hundred Dollars ($100.00) per individual per breach not to exceed a total penalty of One Hundred Thousand Dollars ($100,000.00).

~~C.~~ D. 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.

SECTION 5. AMENDATORY 24 O.S. 2021, Section 166, is amended to read as follows:

Section 166. 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~~ November 1, 2024.

SECTION 6. This act shall become effective November 1, 2024.

59-2-2693 TEK 12/14/2023 2:35:03 PM