

STATE OF OKLAHOMA

1st Session of the 60th Legislature (2025)

SENATE BILL 626

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; updating statutory language; updating statutory references; 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

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

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

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

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

4 5. "Individual" means a natural person;

5 6. "Personal information" means ~~the~~ an individual's first name  
6 or first initial and last name in combination with ~~and linked to~~ any  
7 one or more of the following data elements that relate to ~~a resident~~  
8 ~~of this state, when~~ the individual if any of the data elements are  
9 ~~neither~~ not encrypted, nor redacted, or otherwise altered by any  
10 method or technology in such a manner that the name or data elements  
11 are unreadable or are encrypted, redacted, or otherwise altered by  
12 any method or technology but the keys to unencrypt, unredact, or  
13 otherwise read the data elements have been obtained through the  
14 breach of security:

15 a. social security number,

16 b. driver license number or ~~state~~ other unique  
17 identification card number issued in lieu of a driver  
18 license, or created or collected by a government  
19 entity,

20 c. financial account number, or credit card or debit card  
21 number, in combination with any required expiration  
22 date, security code, access code, or password that  
23 would permit access to ~~the~~ an individual's financial  
24 accounts of a resident account,

1           d. unique electronic identifier or routing code in  
2           combination with any required security code, access  
3           code, or password that would permit access to an  
4           individual's financial account, or

5           e. unique biometric data such as a fingerprint, retina or  
6           iris image, or other unique physical or digital  
7           representation of biometric data.

8 The term does not include information that is lawfully obtained from  
9 publicly available ~~information~~ sources, or from federal, state or  
10 local government records lawfully made available to the general  
11 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  
18           required to provide notice demonstrates that the cost  
19           of providing notice will exceed Fifty Thousand Dollars  
20           (\$50,000.00), or that the affected class of residents  
21           to be notified exceeds one hundred thousand (100,000)  
22           persons, or that the individual or the entity does not  
23           have sufficient contact information or consent to  
24           provide notice as described in subparagraph a, b, or c

1 of this paragraph. Substitute notice consists of any  
2 two of the following:

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

11 8. "Reasonable safeguards" means policies and practices that  
12 ensure personal information is secure, taking into consideration an  
13 entity's size and the type and amount of personal information. The  
14 term includes, but is not limited to, conducting risk assessments,  
15 implementing technical and physical layered defenses, employee  
16 training on handling personal information, and establishing an  
17 incident response plan; and

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

- 21 a. five digits of a social security number, or  
22 b. the last four digits of a driver license number, ~~state~~  
23 unique identification card number created or collected  
24 by a government entity, or account number.

1 SECTION 2. AMENDATORY 24 O.S. 2021, Section 163, is

2 amended to read as follows:

3 Section 163. A. An individual or entity that owns or licenses  
4 computerized data that includes personal information shall ~~disclose~~  
5 provide notice of any breach of the security of the system following  
6 ~~discovery~~ determination or notification of the breach of the  
7 security of the system to any resident of this state whose  
8 unencrypted and unredacted personal information was or is reasonably  
9 believed to have been accessed and acquired by an unauthorized  
10 person and that causes, or the individual or entity reasonably  
11 believes has caused or will cause, identity theft or other fraud to  
12 any resident of this state. Except as provided in subsection D of  
13 this section or in order to take any measures necessary to determine  
14 the scope of the breach and to restore the reasonable integrity of  
15 the system, the disclosure shall be made without unreasonable delay.

16 B. An individual or entity ~~must disclose~~ shall provide notice  
17 of the breach of the security of the system if encrypted or redacted  
18 information is accessed and acquired in an unencrypted or unredacted  
19 form or if the security breach involves a person with access to the  
20 encryption key and the individual or entity reasonably believes that  
21 such breach has caused or will cause identity theft or other fraud  
22 to any resident of this state.

23 C. An individual or entity that maintains computerized data  
24 that includes personal information that the individual or entity

1 does not own or license shall ~~notify~~ provide notice to the owner or  
2 licensee of the information of any breach of the security of the  
3 system as soon as practicable following ~~discovery~~ determination, if  
4 the personal information was or if the entity reasonably believes it  
5 was accessed and acquired by an unauthorized person.

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

13 E. 1. An individual or entity required to provide notice in  
14 accordance with subsection A, B, or C of this section shall also  
15 provide notice to the Attorney General of such breach without  
16 unreasonable delay but in no event more than sixty (60) days after  
17 providing notice to impacted residents of this state as required by  
18 this section. The notice shall include the date of the breach, the  
19 date of its determination, the nature of the breach, the type of  
20 personal information exposed, the number of residents of this state  
21 affected, the estimated monetary impact of the breach to the extent  
22 such impact can be determined, and any reasonable safeguards the  
23 entity employs.

1        2. A breach of a security system where fewer than five hundred  
2 (500) residents of this state are affected within a single breach  
3 shall be exempt from the notice requirements of paragraph 1 of this  
4 subsection.

5        3. A breach of a security system maintained by a credit bureau  
6 where fewer than one thousand (1,000) residents of this state are  
7 affected within a single breach shall be exempt from the notice  
8 requirements of paragraph 1 of this subsection.

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

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

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

16        Section 164. A. An individual or entity that maintains its own  
17 notification procedures as part of an information privacy or  
18 security policy for the treatment of personal information and that  
19 are consistent with the timing requirements of ~~this act~~ the Security  
20 Breach Notification Act shall be deemed to be in compliance with the  
21 notification requirements of ~~this act~~ subsection A, B, or C of  
22 Section 163 of this title if ~~it~~ the individual or entity notifies  
23 residents of this state in accordance with its procedures in the  
24 event of a breach of security of the system.



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

6 1. A financial institution that complies with the notification  
7 requirements prescribed by the ~~Federal~~ Gramm-Leach-Bliley Act and  
8 the federal Interagency Guidance on Response Programs for  
9 Unauthorized Access to Customer Information and Customer Notice ~~is~~  
10 ~~deemed to be in compliance with the provisions of this act.;~~

11 2. An entity that complies with the notification requirements  
12 prescribed by the Oklahoma Hospital Cybersecurity Protection Act of  
13 2023 or the Health Insurance Portability and Accountability Act of  
14 1996 (HIPAA); and

15 3. An entity that complies with the notification requirements  
16 or procedures pursuant to the rules, ~~regulation~~ regulations,  
17 procedures, or guidelines established by the primary or functional  
18 federal regulator of the entity ~~shall be deemed to be in compliance~~  
19 ~~with the provisions of this act.~~

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

22 Section 165. A. A violation of ~~this act~~ the Security Breach  
23 Notification Act that results in injury or loss to residents of this  
24 state may be enforced by the Attorney General or a district attorney

1 in the same manner as an unlawful practice under the Oklahoma  
2 Consumer Protection Act.

3 B. Except as provided in subsection ~~C~~ D of this section, the  
4 Attorney General or a district attorney shall have exclusive  
5 authority to bring an action and may obtain ~~either~~ actual damages  
6 for a violation of ~~this act or~~ the Security Breach Notification Act  
7 and a civil penalty not to exceed One Hundred Fifty Thousand Dollars  
8 (\$150,000.00) per breach of the security of the system or series of  
9 breaches of a similar nature that are ~~discovered~~ determined in a  
10 single investigation. Civil penalties shall be based upon the  
11 magnitude of the breach, the extent to which the behavior of the  
12 individual or entity contributed to the breach, and any failure to  
13 provide the notice required by Section 163 of this title.

14 C. 1. An individual or entity that uses reasonable safeguards  
15 and provides notice as required by Section 163 or 164 of this title  
16 shall not be subject to civil penalties and may use such compliance  
17 as an affirmative defense in a civil action filed under the Security  
18 Breach Notification Act.

19 2. An individual or entity that fails to use reasonable  
20 safeguards but provides notice as required by Section 163 or 164 of  
21 this title shall not be subject to the civil penalty set forth in  
22 subsection B of this section but shall be subject to actual damages  
23 and a civil penalty of Seventy-five Thousand Dollars (\$75,000.00).

1           C. D. A violation of ~~this act~~ the Security Breach Notification  
2 Act by a state-chartered or state-licensed financial institution  
3 shall be enforceable exclusively by the primary state regulator of  
4 the financial institution.

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

7           Section 166. ~~This act~~ The Security Breach Notification Act  
8 shall apply to the ~~discovery~~ determination or notification of a  
9 breach of the security of the system that occurs on or after  
10 ~~November 1, 2008~~ January 1, 2026.

11           SECTION 6. This act shall become effective January 1, 2026.

13           60-1-891           CN           1/19/2025 5:40:17 AM