

§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.

**Comment [1]:** BDERIV

**Comment [2]:** EDERIV