 KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

West's Tennessee Code Annotated
Title 47. Commercial Instruments and Transactions
Chapter 18. Consumer Protection (Refs & Annos)
Part 21. Identity Theft Deterrence

T. C. A. § 47-18-2107

§ 47-18-2107. Breaches of security systems; definitions; notice

Effective: April 4, 2017
Currentness

(a) As used in this section:

(1) "Breach of system security":

(A) Means the acquisition of the information set out in subdivision (a)(1)(A)(i) or (a)(1)(A)(ii) by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder:

(i) Unencrypted computerized data; or

(ii) Encrypted computerized data and the encryption key; and

(B) Does not include the good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder if the personal information is not used or subject to further unauthorized disclosure;

(2) "Encrypted" means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2;

(3) "Information holder" means any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state;

(4) "Personal information":

(A) Means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements:

 © 2018 Thomson Reuters. No claim to original U.S. Government Works.

(i) Social security number;

(ii) Driver license number; or

(iii) Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and

(B) Does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; and

(5) "Unauthorized person" includes an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose.

(b) Following discovery or notification of a breach of system security by an information holder, the information holder shall disclose the breach of system security to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in subsection (d).

(c) Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in subsection (d).

(d) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, it must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation.

(e) For purposes of this section, notice may be provided by one (1) of the following methods:

(1) Written notice;

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 or if the information holder's primary method of communication with the resident of this state has been by electronic means; or

(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), that the affected class of subject persons to be notified exceeds five hundred thousand

 © 2018 Thomson Reuters. No claim to original U.S. Government Works.

(500,000) persons, or the information holder does not have sufficient contact information and the notice consists of all of the following:

(A) Email notice, when the information holder has an email address for the subject persons;

(B) Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and

(C) Notification to major statewide media.

(f) Notwithstanding subsection (e), if an information holder maintains its own notification procedures as part of an information security policy for the treatment of personal information and if the policy is otherwise consistent with the timing requirements of this section, the information holder is in compliance with the notification requirements of this section, as long as the information holder notifies subject persons in accordance with its policies in the event of a breach of system security.

(g) If an information holder discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one (1) time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. § 1681a, and credit bureaus that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

(h) Any customer of an information holder who is a person or business entity, but who is not an agency of this state or any political subdivision of this state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the information holder from further action in violation of this section. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(i) This section does not apply to any information holder that is subject to:

(1) Title V of the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102); or

(2) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.), as expanded by the Health Information Technology for Clinical and Economic Health Act (42 U.S.C. § 300jj et seq., and 42 U.S.C. § 17921 et seq.).

Credits

2005 Pub.Acts, c. 473, § 1, eff. July 1, 2005; 2016 Pub.Acts, c. 692, §§ 1 to 4, eff. July 1, 2016; 2017 Pub.Acts, c. 91, § 1, eff. April 4, 2017.

T. C. A. § 47-18-2107, TN ST § 47-18-2107
Current through end of the 2017 First Regular Session of the 110th Tennessee General Assembly.

 © 2018 Thomson Reuters. No claim to original U.S. Government Works.

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.