Tennessee Code Annotated
Title 47 – Commercial Instruments and Transactions
Chapter 18 – Consumer Protection
Part 21 – Identity Theft

§ 47-18-2107. Release of personal consumer information.

(a) As used in this section, unless the context otherwise requires:

(1) "Breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure;

(2) "Information holder" means any person or business that conducts business in this state, or any agency of the state of Tennessee or any of its political subdivisions, that owns or licenses computerized data that includes personal information; and

(3) (A) "Personal information" 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, when either the name or the data elements are not encrypted

(i) Social security number;

(ii) Driver license number; or

(iii) Account number, credit 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;

(B) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) Any information holder 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 Tennessee 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 (d), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the

data system.

(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 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.

(d) 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.

(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

(3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice, when the information holder has an e-mail address for the subject persons;

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

(C) Notification to major statewide media.

(f) Notwithstanding subsection (e), an information holder 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.

(g) In the event that a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15

U.S.C. § 1681a, 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 the state or any political subdivision of the state, and who is injured by a violation of this section, may institute a civil action to recover damages and to enjoin the person or business entity 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) The provisions of this section shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102.