WEST VIRGINIA CODE: §46A-2A-102

§46A-2A-102. Notice of breach of security of computerized personal information.

(a) An individual or entity that owns or licenses computerized data that includes personal information shall give 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 (e) 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 notice shall be made without unreasonable delay.

(b) An individual or entity must give 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 that the individual or entity does not own or license shall give 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 the entity reasonably believes was accessed and acquired by an unauthorized person.

(d) The notice shall include:

(1) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data;

(2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn:

(A) What types of information the entity maintained about that individual or about individuals in general; and

(B) Whether or not the entity maintained information about that individual.

(3) The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.

(e) 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.

(f) If an entity is required to notify more than one thousand persons of a breach of security pursuant to this article, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined by 15 U.S.C. §1681a (p), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the entity to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to an entity who is subject to Title V of the Gramm Leach Bliley Act, 15 U.S.C. 6801, et seq.

(g) The notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practice Act in 15 U.S.C. §1692a.