CHAPTER 46A. WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT.

ARTICLE 2A. BREACH OF SECURITY OF CONSUMER INFORMATION.

§46A-2A-101. Definitions.

As used in this article:

(1) "Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

(2) "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit.

(3) "Encrypted" means transformation of data through the use of an algorithmic process to into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable.

(4) "Financial institution" has the meaning given that term in Section 6809(3), United States Code Title 15, as amended.

(5) "Individual" means a natural person.

(6) "Personal information" means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted:

(A) Social security number;

(B) Driver's license number or state identification card number issued in lieu of a driver's license; or

(C) Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

(7) "Notice" means:

(A) Written notice to the postal address in the records of the individual or entity;

(B) Telephonic notice;

(C) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, set forth in Section 7001, United States Code Title 15, Electronic Signatures in Global and National Commerce Act.

(D) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed fifty thousand dollars or that the affected class of residents to be notified exceeds one hundred thousand persons or that the individual or the entity does not have sufficient contact information or to provide notice as described in paragraph (A), (B) or (C). Substitute notice consists of any two of the following:

(i) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

(ii) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or

(iii) Notice to major statewide media.

(8) "Redact" means alteration or truncation of data such that no more than the last four digits of a social security number, driver's license number, state identification card number or account number is accessible as part of the personal information.

§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.

§46A-2A-103. Procedures deemed in compliance with security breach notice requirements.

(a) An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies residents of this state in accordance with its procedures in the event of a breach of security of the system.

(b) A financial institution that responds in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this article.

(c) An entity that complies with the notification requirements or procedures pursuant to the rules, regulation, procedures or guidelines established by the entity's primary or functional regulator shall be in compliance with this article.

§46A-2A-104. Violations.

(a) Except as provided by subsection (c) of this section, failure to comply with the notice provisions of this article constitutes an unfair or deceptive act of practice in violation of section one hundred four, article six, chapter forty-six-a of this code, which may be enforced by the Attorney General pursuant to the enforcement provisions of this chapter.

(b) Except as provided by subsection (c) of this section, the Attorney General shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations of this article. No civil penalty shall exceed one hundred fifty thousand dollars per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.

(c) A violation of this article by a licensed financial institution shall be enforceable exclusively by the financial institution's primary functional regulator.

§46A-2A-105. Applicability.

This article shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this article.