

Publications

June 01, 2014

SECURITY BREACH NOTIFICATION CHART - West Virginia

W. VA. Code § 46A-2A-101 et seq.

S.B. 340 (signed into law March 27, 2008)

Effective June 6, 2008

Application. An individual, government entity, or any other legal entity, whether for profit or not for profit, (collectively, Entity) that owns or licenses computerized data that includes PI.

Security Breach Definition. Unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of PI maintained by an Entity as part of a database of PI regarding multiple individuals and that causes the Entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of WV.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the Entity is not a breach of the security of the system, provided that the PI is not used for a purpose other than a lawful purpose of the Entity or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall give notice of any breach of the security of the system to any resident of WV whose unencrypted and unredacted PI 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 WV.

- An 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 Entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 persons of a breach of security pursuant to this article, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies 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 PI of breach notice recipients.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the 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 PI was or the Entity reasonably believes was accessed and acquired by an unauthorized person.

Timing of Notification. Except 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.

Personal Information Definition. 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 WV, when the data elements are neither encrypted nor redacted:

- Social Security number;
- Driver's license number or state identification card number issued in lieu of a driver's license; or
- Account number, credit card number, 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.

PI 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.

Notice Required. The notice shall include:

- To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired;
- 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 what types of information the Entity maintained about that individual or about individuals in general and whether or not the Entity maintained information about that individual; and
- 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.

Notice may be provided by one of the following methods:

- Written notice to the postal address in the records of the Entity;
- Telephonic notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. If an Entity demonstrates that the cost of providing notice will exceed \$50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the Entity does not have sufficient contact information to provide notice. Substitute notice consists of any two of the following:

- Email notice, if the Entity has email addresses for the members of the affected class of residents;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; or
- Notice to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of PI 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 the Entity notifies residents of WV in accordance with its procedures in the event of a breach of security of the system.

Exception: Compliance with Other Laws.

- **Federal Interagency Guidance.** 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.
- **Primary Regulator.** 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.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice required by this section may be delayed if a law enforcement agency determines and advises the 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.
- Attorney General Enforcement.