Pennsylvania Statutes
Title 73 – Trade and Commerce
Chapter 43 – Breach of Personal Information Notification Act

§ 2301. Short title. This act shall be known and may be cited as the Breach of Personal Information Notification Act.

§ 2302. Definitions. The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

"Encryption." The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

"Individual." A natural person.

"Notice." May be provided by any of the following methods of notification:

(1) Written notice to the last known home address for the individual.

(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.

(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

(4) (i) Substitute notice, if the entity demonstrates one of the following:

(A) The cost of providing notice would exceed $ 100,000.

(B) The affected class of subject persons to be notified exceeds 175,000.

(C) The entity does not have sufficient contact information.

(ii) Substitute notice shall consist of all of the following:

(A) E-mail notice when the entity has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.

(C) Notification to major Statewide media.

"Personal information."

(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

(i) Social Security number.

(ii) Driver's license number or a State identification card number issued in lieu of a driver's license.

(iii) Financial 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.

(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

"Records." Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

"Redact." The term includes, but is not limited to, alteration or truncation 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 data.

"State agency." Any agency, board, commission, authority or department of the Commonwealth and the General Assembly.

§ 2303. Notification of breach.
(a) GENERAL RULE.-- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

(b) ENCRYPTED INFORMATION.-- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

(c) VENDOR NOTIFICATION.-- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

§ 2304. Exceptions. The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

§ 2305. Notification of consumer reporting agencies. When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

§ 2306. Preemption. This act deals with subject matter that is of Statewide concern, and it is the intent of the General Assembly that this act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this Commonwealth regarding the matters expressly set forth in this act.

§ 2307. Notice exemption.
(a) INFORMATION PRIVACY OR SECURITY POLICY.-- An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(b) COMPLIANCE WITH FEDERAL REQUIREMENTS.--

> (1) A financial institution that complies with the notification requirements 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 act.
>
> (2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this act.

§ 2308. Civil relief. A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L. 1224, No. 387), known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

§ 2329. Applicability. This act shall apply to the discovery or notification of a breach in the security of personal information data that occurs on or after the effective date of this section.