Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Pennsylvania

73 Pa. Stat. § 2301 ***et seq.***

S.B. 712 (signed into law Dec. 22, 2005, Act No. 94)

Effective June 20, 2006

S.B. 696 (signed into law Nov. 3, 2022, Act. No. 151)

Effective May 2, 2023

S.B. 824 (signed into law June 28, 2024, Act No. 33)

Effective September 26, 2024

Application. Any state agency, political subdivision, or an individual or a business (collectively, Entity) doing business in PA that maintains, stores, or manages computerized data that includes PI of PA residents.

Security Breach Definition. Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of PI maintained by the Entity as part of a database of PI regarding multiple individuals and that causes or the Entity reasonably believes has caused or will cause loss or injury to any resident of PA.

- Good-faith acquisition of PI 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 PI is not used for a purpose other than the lawful purpose of the Entity and is not subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall provide notice of any breach of the security of the system to any individual whose principal mailing address, as reflected in the computerized data that is maintained, stored, or managed by the Entity, is in PA and whose unencrypted and unredacted PI was or is reasonably believed to have been accessed and acquired by an unauthorized person.

- 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.

Notification to Attorney General. Any Entity required to notify more than 500 Pennsylvania residents must concurrently provide notice to the Attorney General of the breach. Notice must include:

- The organization name and location;
- The date of the breach of the security of the system;
- A summary of the breach incident;
- An estimated total number of individuals affected by the breach; and
- An estimated total number of Pennsylvania affected by the breach.

Notification to Consumer Reporting Agencies. When an Entity provides notification under this act to more than 500 persons at one time, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and number of notices.

Credit Monitoring Services and Providing Free Credit Report. If a breach of security has occurred and the Entity reasonably believes that the data accessed includes an individual's first name and last name or an individual's first initial and last name, in combination with (i) Social Security number, (ii) bank account number, or (iii) driver's license or state ID number, the Entity must also:

- Offer affected individuals credit monitoring services at no cost for a period of 1 year.
- Assume all costs and fees in providing the affected individuals access to one independent credit report from a consumer reporting agency if the individual is not eligible to obtain an independent credit report from a consumer reporting agency for free under 15 U.S.C. § 1681.

If these requirements are triggered, the no-cost services must be described in the individual notification.

Third-Party Data Notification. An Entity that maintains, stores, or manages computerized data on behalf of another Entity shall provide notice of any breach of the security system following discovery to the Entity on whose behalf it maintains, stores or manages the data.

Timing of Notification. Except 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.

Personal Information Definition. 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:

- Social Security number;
- Driver's license number or state identification card number issued in lieu of a driver license;
- 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 an individual's financial account;
- Medical Information in the possession of a State agency or State agency contractor;
- Health Insurance Information; or
- User name or email address in combination with a password or security questions and answers that would permit access to an online account.

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

Notice Required. Notice may be provided by any of the following methods:

- Written notice to the last known home address for the individual;
- 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 PI but does not require the customer to provide PI, and the customer is provided with a telephone number to call or a website to visit for further information or assistance; or
- Email notice, if a prior business relationship exists and the Entity has a valid email address for the individual.

For online account credentials: Notice may be provided in electronic form that directs the individual to promptly change his or her password and security question or answer, or to take other appropriate steps to protect the online account with the entity or other online accounts involving the same login credentials.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $100,000, the affected class of subject persons to be notified exceeds 175,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has an email address for the subject persons;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification 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 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.

Exception: Compliance with Other Laws.

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

Exception: Entities Subject to Insurance Data Security Act. An Entity that is subject to the requirements of the Pennsylvania Insurance Data Security Act (40 PA. C.S. CH. 45) is exempt from notice requirements to the Attorney General.

Other Key Provisions:

- **Delay for Law Enforcement.** Notification required may be delayed if a law enforcement agency determines and advises the Entity in writing, specifically referencing the statute, that the notification will impede a criminal or civil investigation. The required notification shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.
- **Attorney General Enforcement.** The Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of the statute.