Publications
June 01, 2014

# SECURITY BREACH NOTIFICATION CHART - Maryland

**Md. Code Com. Law § 14-3501** ***et seq.***

H.B. 208 (signed into law April 3, 2007)

Effective January 1, 2008

H.B. 974 (signed into law May 4, 2017)

Effective January 1, 2018

H.B. 962 (signed into law May 29, 2022)

Effective October 1, 2022

---

**Application.** Any business entity, whether or not organized to operate at a profit, (collectively, Entity) that owns, maintains, or licenses computerized data that includes PI of an individual residing in MD.

**Security Breach Definition.** The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the PI maintained by an Entity.

- A good-faith acquisition of PI by an employee or agent of an Entity for the purposes of the business, provided that the PI is not used or subject to further unauthorized disclosure, does not constitute a security breach.

**Notification Obligations.** An Entity that discovers or is notified of a breach of the security of the system, shall notify the individual of the breach.

- Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines that the PI of the individual was not and will not be misused as a result of the breach. If, the Entity determines that notification is not required, the Entity shall maintain records that reflect its determination for 3 years after the determination is made. If, after the investigation is concluded, the Entity determines that the breach of the security of the system creates a likelihood that PI has been or will be misused, the business shall notify the individual of the breach.

**Attorney General Notification.** Prior to giving the notification required under the statute, an Entity shall provide notice of a breach of the security of a system to the state Office of the Attorney General, and the notice shall include, at a minimum:

- The number of affected individuals residing in the State;
- A description of the breach of the security of a system, including when and how it occurred;
- Any steps the business has taken or plans to take relating to the breach of the security of a system; and
- The form of notice that will be sent to affected individuals and a sample notice.

**Notification to Consumer Reporting Agencies.** If an Entity must notify 1,000 or more individuals, the Entity also shall notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

**Third-Party Data Notification.** An Entity that maintains PI of MD residents that the Entity does not own or license shall notify the owner or licensee of the PI of a breach of the security of the system if it is likely that the breach has resulted or will result in the misuse of PI of an individual residing in MD.

- Notification required by a third-party Entity shall be given as soon as practicable but not later than 45 days after the Entity discovers or is notified of the breach of the security of a system.
- A third-party Entity shall share with the owner or licensee information relative to the breach.

**Timing of Notification.** As soon as reasonably practicable, but no later than 45 days after the business concludes the investigation, consistent with measures necessary to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

**Personal Information Definition.**

1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

- Social Security number, individual taxpayer identification number, passport number, or other identification number issued by the federal government;
- Driver's license number or state identification card number;
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;
- Health information, including information about an individual's mental health;
- Health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or
- Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account.
- Genetic information of an individual

2) A username or email address in combination with a password or security question and answer that permits access to an individual's email account.

"Encrypted" means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.

PI does not include (i) publicly available information that is lawfully made available to the general public from federal, state, or local government records; (ii) information that an individual has consented to have publicly disseminated or listed; or (iii) information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).

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

- Written notice sent to the most recent address of the individual in the records of the business;
- Telephonic notice, to the most recent telephone number of the individual in the records of the business; or
- Email to the most recent email address of the individual in the records of the business, if the individual has expressly consented to receive email notice.

*Generally:* Except for breaches involving loss of information that permits access to an email account only, notification shall include:

- To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of PI were, or are reasonably believed to have been acquired;
- Contact information for the business making the notification, including the business's address, telephone number, and toll-free telephone number if one is maintained;
- The toll-free telephone numbers and addresses for the major consumer reporting agencies; and
- The toll-free telephone numbers, addresses, and website addresses for (i) the Federal Trade Commission and (ii) the state Attorney General, along with a statement that the individual can obtain information from these sources about steps the individual can take to avoid identity theft.

*For email account credentials only:* the Entity may provide notice in electronic or other form that directs the individual whose PI has been breached promptly to:

- Change the individual's password and security question or answer, as applicable; or
- Take other steps appropriate to protect the email account with the business and all other online accounts for which the individual uses the same username or email and password or security question or answer.

The notification may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected email account from an IP address or online location from which the business knows the individual customarily accesses the account, but otherwise may not be given to the individual by sending notification by email to the email account affected by the breach.

**Substitute Notice Available.** If the Entity demonstrates that the Entity does not have sufficient contact information to give notice. Substitute notice shall consist of all of the following:

- Email notice to an individual entitled to notification, if the business has an email address for the individual to be notified;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains a website; and
- Notification to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

**Exception: Compliance with Other Laws.**

- **Primary Regulator.** An Entity that complies with the requirements for notification procedures, the protection or security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by the primary or functional federal or state regulator of the Entity shall be deemed to be in compliance with the statute.
- **Gramm-Leach-Bliley Act.** An Entity or the affiliate of an Entity that is subject to and in compliance with the Gramm-Leach-Bliley Act, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle.

- An Entity or affiliate of the Entity that is in compliance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed to be in compliance.

**Other Key Provisions:**

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable but no later than 7 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security if (i) the original 45 day period has already elapsed, or (ii) the end of the original 45 day period, or (iii) 7 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.
- **Attorney General Enforcement.**
- **Private Right of Action.** Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.
- Waiver Not Permitted.