Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Delaware

Del. Code Ann. tit. 6 § 12B-101 ***et seq.***

H.B. 116 (signed into law June 28, 2005)

Effective June 28, 2005

H.B. 247 (signed into law June 10, 2010)

Effective June 10, 2010

House Substitute 1 for HB 180 (signed into law August 17, 2017)

Effective April 14, 2018

Application. Any person, legal or commercial entity, or government agency who conducts business in DE (collectively, Entity) and who owns or licenses computerized data that includes PI.

Security Breach Definition. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI. The unauthorized acquisition of encrypted data is not a breach, unless such unauthorized acquisition includes, or is reasonably believed to include, an encryption key that could render the PI readable or useable.

- 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 an unauthorized purpose or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall provide notice of any breach of security following determination of the breach of security to any resident of DE whose PI was breached or is reasonably believed to have been breached.

- Notification is not required if after an appropriate investigation the Entity reasonably determines that the breach of security is unlikely to result in any harm to the individuals whose PI has been breached.

Attorney General Notification. If the number of DE residents to be notified exceeds 500 residents, the Entity shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General.

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 and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following determination of the breach of security. Cooperation includes sharing with the owner or licensee information relevant to the breach.

Timing of Notification. Without unreasonable delay but not later than 60 days after determination of the breach of security.

- If the Entity cannot, through reasonable diligence, identify within 60 days that the PI of certain DE residents was included in a breach of security, the Entity must provide notice as soon as practicable after the determination that the breach of security included the PI of such residents, unless the Entity provided substitute notice.

Personal Information Definition. A DE resident's first name or first initial and last name, in combination with any one or more of the following data elements:

- Social Security number;
- Driver's license number or state or federal identification card number;
- 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 account;
- Passport number;
- Username or email address, in combination with a password or security question and answer that would permit access to an online account;
- Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid (DNA) profile;
- Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person;
- Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes; or
- An individual taxpayer identification number.

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

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

- Written notice;
- 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) or if the person's primary means of communication with the resident is by electronic means.

For email account credentials: For breaches of login credentials for an email account furnished by the Entity, notice may not be provided to the breached email address, but may be provided via methods otherwise permitted, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the person knows the resident customarily accesses the account.

Credit Monitoring Services. If the breach of security includes Social Security numbers, the Entity shall offer to each resident whose Social Security number was affected, credit monitoring services at no cost to such resident for a period of 1 year. The Entity shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on his or her credit file.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice will exceed $75,000, or that the number of DE residents to be notified exceeds 100,000, or the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following:

- Email notice, if the Entity has email addresses for the members of the affected class of DE residents;

- Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one; and
- Notice to major statewide media, including newspapers, radio, television, and publications, on the major social media platforms of the person providing notice.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of the statute, is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected DE residents in accordance with its policies in the event of a breach of the security of the system.

Exception: Compliance with Other Laws.

- **Primary Regulator.** An Entity is deemed in compliance with this chapter if:
  - it is regulated by state or federal law, including HIPAA or GLBA;
  - it maintains procedures for a breach of security pursuant to requirements established by its primary or functional state or federal regulator; and
  - it notifies affected DE residents in accordance with the maintained procedures.

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. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- **Attorney General Enforcement.** The Attorney General may bring an action to address violations of this chapter and for other relief that may be necessary to ensure compliance and recover direct economic damages.