Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - New Jersey

N.J. Stat. § 56:8-161 ***et seq.***

A. 4001 (signed Sept. 22, 2005)

Effective January 1, 2006 (all provisions except those governing police reports, which are effective on Sept. 22, 2005)

Senate Bill No. 52 (signed into law May 10, 2019)

Effective September 1, 2019

Application. Any government, or other entity, however organized and whether or not organized to operate at a profit, that conducts business in NJ (collectively, Entity), that compiles or maintains computerized records that include PI.

Security Breach Definition. Unauthorized access to electronic files, media or data containing PI that compromises the security, confidentiality, or integrity of PI when access to the PI has not been secured by encryption or by any other method or technology that renders the PI unreadable or unusable.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate business purpose is not a breach of security, provided that the PI is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall disclose any breach of security of computerized records following discovery or notification of the breach to any customer who is a resident of NJ whose PI was, or is reasonably believed to have been, accessed by an unauthorized person.

- Disclosure of a breach of security to a customer shall not be required if the Entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for 5 years.

Notification to Consumer Reporting Agencies. If an Entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Attorney General/Police Notification. Any Entity required under this section to disclose a breach of security of a customer's PI shall, prior to disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

Third-Party Data Notification. An Entity that compiles or maintains computerized records that include PI on behalf of another Entity shall notify that Entity of any breach of security of the computerized records

immediately following discovery, if the PI was, or is reasonably believed to have been, accessed by an unauthorized person.

Timing of Notification. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name linked with any one or more of the following data elements:

- Social Security number;
- Driver's license number or state identification card number; 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 an individual's financial account.
- Username, email address, or any other account holder identifying information, in combination with any password or security question and answer that would access to an online account.

Dissociated data that, if linked, would constitute PI is PI if the means to link the dissociated data were accessed in connection with access to the dissociated data. PI shall 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; 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).
- For breaches involving online account credentials only, in "electronic or other form."
- Except for breaches involving credentials for an email account, which must be provided via written notice or via online delivery when the customer is connected to the online account from an IP address or online location from which the business or public entity knows the customer customarily accesses the account.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject individuals to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has email addresses;
- 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 security policy for the treatment of PI and is otherwise consistent with the requirements of the statute, shall be deemed in compliance with the notification requirements of the statute if it notifies subject customers in accordance with its policies in the event of a breach of security of the system.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed.