Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - New York

N.Y. Gen. Bus. Law § 899-aa

A.B. 4254 (signed into law August 10, 2005)

N.Y. State Tech. Law § 208

Effective December 7, 2005

S. 2605-D (signed into law March 28, 2013)

Effective March 28, 2013

S. 5575B (signed into law July 25, 2019)

Effective October 23, 2019

Application. Any person, business, or state entity (excepting the judiciary, cities, counties, municipalities, villages, towns, and other local agencies) (collectively, Entity) that conducts business in New York State and that owns or licenses computerized data that includes private information.

Security Breach Definition. Unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business.

In determining whether information has been accessed, or is reasonably believed to have been accessed, Entities may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, Entities may consider the following factors, among others:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
- Indications that the information has been downloaded or copied; or
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Good-faith access to or acquisition of private 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, provided that the private information is not used or subject to unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security following discovery or notification of the breach in the security of the system to any resident of NY whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

Notice to affected persons is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the Entity reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. This determination must be documented in writing and maintained for at least 5 years. If more than 500 NY residents are affected, the Entity shall provide the written determination to the state Attorney General within ten days after the determination.

Notification to Consumer Reporting Agencies. If more than 5,000 NY residents are to be notified at one time, the Entity shall also notify consumer reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected persons.

Attorney General/Agency Notification. If any NY residents are to be notified, the Entity shall notify the state Attorney General, the department of state consumer protection board, and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template notice sent to affected persons. The state AG's website has a form to be used for notifications.

- Any Covered Entity required to provide notification of a breach, including breach of information that is not "private information" as defined herein, to the Secretary of Health and Human Services pursuant to HIPAA or the HITECH Act, shall provide such notification to the state Attorney General within 5 days of notifying the Secretary.

Third-Party Data Notification. Any Entity that maintains computerized data that includes private information that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

Timing of Notification. The disclosure 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 system.

Personal Information Definition. Information concerning a natural person that, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

Private Information Definition. Personal information consisting of:

(1) any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

- Social Security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

- Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or

(2) A username or email address in combination with a password or security question and answer that would permit access to an online account.

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

- NY's statute uses the term "private information" the same way most statutes use "personal information," and separately defines "personal information" to mean all identifiable information about a person. The latter term is used only to require that notices include *all* types of personal *and* private information that has been exposed.

Notice Required. Notice shall include:

- Contact information for the Entity making the notification;
- The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information; and
- A description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

The notice required shall be directly provided to the affected persons by one of the following methods:

- Written notice;
- Telephonic notice, provided that a log of each such notification is kept by the Entity; or
- Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the Entity who notifies affected persons in such form; provided further, however, that in no case shall any Entity require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

Substitute Notice Available. If the Entity demonstrates to the state Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons 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 for the subject persons, except if the breached information includes an email address in combination with a password or security question and answer that would permit access to the online account, in which case the Entity shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the Entity knows the consumer customarily uses to access the online account;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Compliance with Other Laws. If notice of the breach of the security of the system is made pursuant to any of the following laws, nothing in this statute shall require separate notice to affected individuals,

but notice must still be provided to the regulators noted above and the consumer reporting agencies.

- Regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (GLBA)
- Regulations implementing the Health Insurance Portability and Accountability Action of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)
- Part 500 of Title 23 of the Code of the State of New York (NY DFS Cybersecurity Regulation)
- Any other data security rules and regulations of, and the statutes administered by, any official department, division, commission, or agency of the federal or New York state government.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
- **Attorney General Enforcement.** The Attorney General may bring an action to enjoin and restrain the continuation of such violation.